
CYBER DEFENSE
MAGAZINE
WHERE INFOSEC KNOWLEDGE IS POWER
2020
SPECIAL
EDITION
RSAConference
Where the world
talks security

Welcome to CDM's RSA Conference 2020 Special Edition

Traditionally, the monthly issues of Cyber Defense Magazine (CDM) carry welcome messages from the Publisher and the Editors. For this RSA Conference 2020 Special Edition, in my capacity as U.S. Editor-in-Chief, I have the honor of posting an integrated welcome message from all of us. With that, a tip of the hat is in order to Gary Miliefsky, our Publisher, and to Pierluigi Paganini, International Editor-in-Chief.

We are pleased to support and participate in RSA Conference 2020 as they focus on the Human Element. In particular, we endorse the drive to expand educational opportunities for those in pursuit of a career in cybersecurity.

CDM recognizes this initiative in response to two documented trends in cybersecurity: (1) the continued growth in reported data breaches and other cyber exploits; and (2) growth in the shortage of degreed and certified cybersecurity professionals to meet the positions opening in the field.

As reported by many experts in cybersecurity and more granularly by our publisher, Gary Miliefsky:

"*4.2 million 387 thousand 991 cybersecurity jobs will remain unfilled, globally, by then end of next year, 2021. In parallel, cyber attackers are improving their skills, leveraging new artificial intelligence tools and automation, making the threat landscape even more dangerous than ever.…"*

We dedicate this issue to meeting the needs of the cyber defense community, especially in communication, information, and education. In so doing, CDM is also laying the foundation to serve as a robust resource for academic institutions offering degrees in cybersecurity and their students.

In the coming months, CDM will bring a closer focus to ways in which vendors and clients alike can benefit from a growing cadre of cybersecurity professionals. With over 5 million individual inquiries per month, CDM is the leading publication for cybersecurity endeavors.

One of the successful ways CDM has brought attention to the leaders in cybersecurity is the Infosec Awards program: https://cyberdefenseawards.com/ and many high profile executive interviews at https://www.cyberdefensetv.com and https://www.cyberdefenseradio.com/

We have much exciting news to share with you, in the coming months and some very big news in early March so stay tuned and keep our home page bookmarked and frequently visited and shared at https://www.cyberdefensemagazine.com

We would be remiss if we did not draw attention to CDM's "Green" initiative for the 8th Annual RSA Conference Edition.

Wishing you all success in your cyber security endeavors,

Yan Ross
U.S. Editor-in-Chief
Cyber Defense Magazine

About the Editor

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemediagroup.com

Contents

CYBER DEFENSE MAGAZINE
is a Cyber Defense Media Group (CDMG) publication distributed electronically via opt-in GDPR compliance-Mail, HTML, PDF, mobile and online flipbook forwards. All electronic editions are available for free, always. No strings attached. Annual EDITIONs of CDM are distributed exclusively at the RSA Conference each year for our USA editions and at IP EXPO EUROPE in the UK for our Global editions. Key contacts:

PUBLISHER
Gary S. Miliefsky
garym@cyberdefensemagazine.com

PRESIDENT
Stevin V. Miliefsky
stevinv@cyberdefensemagazine.com

V.P. INTERNATIONAL BIZ DEV & STRATEGY
Tom Hunter
tom@cyberdefensemediagroup.com

V.P. US/CANADA/LATAM BIZ DEV & STRATEGY
Olivier Vallez
olivier.vallez@cyberdefensemagazine.com

EDITOR-IN-CHIEF
Yan Ross
yan.ross@cyberdefensemediagroup.com

MARKETING, ADVERTISING & INQUIRIES
marketing@cyberdefensemagazine.com
Interested in writing for us:
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: +1-833-844-9468
International: +1-603-280-4451
New York (USA/HQ): +1-646-586-9545
London (UK/EU): +44-203-695-2952
Hong Kong (Asia): +852-580-89020
Skype: cyber.defense
E-mail: marketing@cyberdefensemagazine.com
Awards: www.cyberdefenseawards.com
Radio: www.cyberdefenseradio.com
TV: www.cyberdefensetv.com
Web: www.cyberdefensemagazine.com

To Reach Us Via US Mail:
Cyber Defense Magazine
276 Fifth Avenue, Suite 704
New York, NY 10001
EIN: 454-18-8465
DUNS# 078358935

Welcome to CDM's RSA Conference 2020 Special Edition

The past year has gone by in the blink of an eye, and here we are again only weeks away from RSA Conference 2020 running from February 24-28. We're very much looking forward to welcoming nearly 45,000 security professionals, media, analysts and vendors in San Francisco at our 29th annual Conference, where people from all around the world come together to talk security.

For nearly three decades, the Conference has served as a hub for the cybersecurity industry, bringing together a wide array of professionals across all sectors and industries. This year's theme, Human Element, has created lots of buzz, and we saw an increased number of high quality submissions from speakers who thought about everything from product security to artificial intelligence. From this pool, we pulled together an impressively diverse and richly informative agenda comprised of more than 20 tracks. Between the West and South Stage keynotes, we have some of the most esteemed leaders who will inspire, inform and motivate this year's attendees to think more deeply about the relationship between humans and technology.

You'll also see two new technical tracks focused on Product Security and Community Open Source Tools. As we identified in our 2020 Trends Report, the Human Element extends far beyond security awareness. Even those sessions that focus on risk management, cloud security, protecting data and the supply chain, DevSecOps, and security strategy and architecture touch upon the Human Element. This year's Conference is all about tapping into a place of collective strength to maximize our human potential to build a more secure world.

The cybersecurity industry is comprised of incredibly brilliant and talented individuals who are dedicated to sharing their expertise, and RSA Conference continues to empower that human desire to contribute to the collective good. In response to requests for more networking opportunitites at Conference, we've introduced the new RSAC Engagement Zone, where attendees can participate in a variety of interactive learning sessions from Cooperative Learning and Problem Solving, to Birds of a Feather, Speed Networking and Braindate. Last year, we added the RSAC CISO Boot Camp, where senior-level security executives were able to come together and focus on solving the industry's biggest issues and we've expanded it this year to provide advanced offerings for the seasioned CISO.

Throughout 2019, we had a chance to reflect on answers to the question of how can we make cybersecurity better, and we know that in large part security cannot be better without the Human Element. That's why so much of what RSAC 2020 has to offer is a blending of the human and the technical so that we can ensure product security as we all move forward on our digital transformation journeys.

As technology and innovation continue to drive changes in the world around us, we must keep pace with those changes and prepare for the reality that to err is human. Nothing about cybersecurity is impervious, but when we value people as much as technology, we can better prepare for, and defend against, cyber threats by intertwining the resilence of the human spirit into the important work that we do with technology.

We look forward to seeing you at RSAC this year.
Linda Gray Martin
Sr. Director & General Manager, RSA Conference

RSA® Conference | Where the world talks security

Peanut Butter + Jelly
Movies + Popcorn
File Transfer + OpenPGP

OpenPGP is a popular encryption standard that's used by banks, financial institutions, healthcare organizations and other highly regulated industries to protect the privacy and integrity of sensitive files.

GoAnywhere OpenPGP Studio is a free PGP file encryption tool that makes it easy to protect your sensitive files while complying with the OpenPGP standard. It uses a safer dual-key (asymmetric) system and allows you to:

- Encrypt, decrypt, and sign files
- Verify digital signatures
- Compress output files
- Manage public and private PGP keys

Download OpenPGP Studio at ***www.goanywhere.com/openpgp-studio*** and get started with free desktop file encryption today.

GO ANYWHERE®
A HelpSystems Solution

How Organizations Can Achieve True Zero-Knowledge Security for Their Secrets Management

By Oded Hareven, CEO and Co-Founder of AKEYLESS

Available solutions for secrets and keys management mostly fail in hybrid and multi-cloud environments. The AKEYELSS SaaS platform stands to change that.

Organizations are moving their secrets and keys from on-prem to the cloud, and in very high rates. It makes sense; everything else is being moved to a cloud environment. Cloud service providers, chiefly AWS, Azure and GCP, offer their own secrets management solutions, and many CISOs are forced to opt in for this because they have no other better solution and because again, it makes sense - what can be safer than a provider's own native solution?

But with hybrid cloud architecture, most organizations find themselves dealing with multiple environments, and thousands of containers and microservices. Since many more machine-to-machine components need to communicate with one another, and since these components require access management by administrators, a significantly higher number of secrets is accumulating. Especially since the scale has tipped - more and more machines - secrets and keys have become a major security vulnerability that should be addressed by security teams.

What Are Secrets and How They Are Used

Secrets are data items of authentication and authorization, such as passwords, API Tokens, TLS Certificates, SSH Keys, Encryption Keys, Signing Keys and others. Both machines and humans use secrets to authenticate and communicate.

Managing and protecting the increasing amount of secrets has become a glaring pain point for CISOs. The reason for that lies in the sprawling nature that secrets are placed for 'safe keeping'; in code, scripts, various infrastructures and development stages, thus posing a real risk if mismanaged and unprotected. There's more: Secrets kept in cloud platforms that perform CI/CD are required, by their nature, to manage other machines and need to store secrets to allow access. And, more often than not, signing keys (used for sealing code and software updates) are kept in non-secure location, such as the programmer's station or build servers.

Note that most of the 'safe keeping' places mentioned above are actually not secure in any way. And as a wide range of secret types are placed in multiple cloud infrastructures, private and public, the threat intensifies.

How Are Organizations Handling Secrets Management Today

Basically in two ways, either using a self-deployed solution, on-prem or in the cloud, or using the cloud provider's in-house solution. Both pose their own operational challenges and security risks.

Self-Deployed Solution

Deploying a secrets management solution is a rigorous and costly effort for any organization. It might be a suitable solution for new or smaller-scale companies that operate in a single, narrow environment, but it gets immediately more complex to manage and maintain when organizations reach their second environment, either on the cloud or a hybrid one, not to mention across various geographical locations; troubles begin with replications and synchronizations.

A very special skill set is required to support a complex environment, especially when the aim is to provide a comprehensive solution for all the various secret types, of machines and humans, since it requires operating various products. Also, unique knowledge is needed for the fast implementation, deployment and maintenance of such a complex architecture that might include a credentials valuating solution that supports multiple connectors for many types of platforms, such as SSH and privileged access control, PKI certificates automation solution and encryption keys' management platform.

CSP Solution

The other available way to deal with secrets management today is to go with the cloud service provider's own in-house solution. Before getting into the operational limitations and challenges that a CSP solution poses, the Closed Garden issue should be addressed. Cloud provides, quite intentionally, offer excellent services and support for their own infrastructure but fail to offer adequate solutions for cross-cloud operations; AWS' secrets management solution would prove problematic working across Azure, or even on-prem.

For a small-to-medium, cloud-born company that works with a single cloud provider in a single region and conducts all its operations in that cloud, this would be a reasonable solution. Moving on to the vast majority of companies and larger organizations that operate in multi-cloud and/or multi-region and/or hybrid environments, these aren't fully supported by individual cloud providers. On top of that,

not all services and features of the mega cloud providers are supported in every region. A patchwork of workarounds and compromises are needed to be put in place in order to continue using a CSP secrets management solution in non-native environments.

Above all, when using a CSP-native secrets management solution, organizations are compromising their security in one significant way - cloud providers have access to their secrets. This security flow is often overlooked but shouldn't be. This is not to say that Amazon or Microsoft are plotting to steal your secrets, but rather that your organization's most sensitive data is exposed to insider threats and malicious attacks through an additional entry point. More than that, according to cloud providers' declared Shared Responsibility Model, they are responsible for infrastructure security while you, the user, is required to take measures to secure your own data stored on the cloud, including your secrets and encryption keys.

What Would Be the Ideal Solution for Secrets Management

An ideal secrets management solution would be one that solves all the faults of self-deployed solutions and cloud providers' native solutions.

A solution that can manage any secret in any environment and allows for dynamic scaling. It should be a single solution that centralizes the decentralized business of managing secrets and keys. It should work, seamlessly and simply, in multi-cloud and hybrid environments and be able to handle endless infrastructures of semiservices and containers, no matter in what architecture they are sprawled, all while supporting every use case to unify all secrets and keys management components, used by either machines or humans.

Most importantly and above all, it should provide zero-knowledge security to the organization; for managing its most sensitive data, nothing less should be acceptable. What is the most sensitive data? Encryption keys, so it is essential to ensure that no one but you has visibility or access to them.

Is it at all possible to achieve zero-knowledge when it comes to encryption keys? In order to achieve zero-knowledge when keeping your keys at a third-party vendor (and maintain complete ownership over them), a solution is required where the provider is unable to see or access the keys cryptographically.

Fragmented keys are a common practice. A key isn't kept in a single location, but broken to pieces, making it more difficult to obtain the entire key. But, at the moment of encryption, or decryption, the key is assembled in order to lock or unlock. And at that moment, the key in its entirety is visible and accessible to malicious attacks by proxy of the cloud provider.

Zero-Knowledge in secrets and keys management seems be unattainable and indeed it was, until now. A new technology, DFC™ - Distributed Fragments Cryptography - by AKEYLESS, is enabling the use of fragmented encryption keys without ever needing to assemble them. More than that, DFC™ places key fragments in various locations, constantly refreshed mathematically and lets the user keep one fragment of the key in his own environment. True Zero-Knowledge is achieved - the Encryption Key never exists as a whole AND even AKEYLESS, the service provider, can't see or access the key as a whole.

AKEYLESS Secrets Management Platform Answers All Your Needs with a Single Solution

- Provides a unified, centralized solution that supports all types of secrets: encryption keys, API-keys, tokens, passwords (SQL, LDAP), SSH keys, x.509 certificates, signing Keys
- Seamlessly supports any configuration, in both hybrid and multi-cloud environments in all regions
- A cloud-native SaaS solution that ensures exclusive ownership of organizations over their security by denying its own access to their secrets and keys
- Requires no installation and enables deployment within minutes
- Plugs into every common cloud platform such as Kubernetes, Docker, Jenkins, Terraform, Ansible, and others
- Flexible pay-per-use model makes it completely scalable and affordable
- Patent-pending, Zero-Knowledge technology DFC™ - Distributed Fragments Cryptography - enables a unique protection to any secret, giving only its owner the exclusive ability to access, encrypt and decrypt it
- FIPS 140-2 certified, recognized worldwide as one of the highest standards for cryptography validation

AKEYLESS is a real game changer for securing data on the cloud with its DFC™-powered SaaS platform. It offers a singular solution to a growing problem - managing secrets and keys across hybrid and multi-cloud environments, and as such it solves for developers and DevOps the challenge of scaling.

For CISOs, it solves a consisting headache - can I really trust a SaaS solution? With AKEYLESS, organizations finally don't need to compromise scalability nor security when moving to multi-cloud or hybrid environments. This is exactly where AKEYLESS brings the utmost value to CISOs.

About the Author

Oded Hareven is the CEO and Co-Founder of AKEYLESS, a cloud-native, zero-knowledge secrets management platform. AKEYLESS' mission is to enable organizations to fully protect and automatically manage any type of secret, in any environment - hybrid or multi cloud.

Oded, a veteran of the Israeli IDF cyber technology elite unit, held various senior product and project management positions and is an expert in product development for the cyber security industry. Learn more about Oded Hareven https://www.akeyless.io/

From unstructured data to actionable intelligence for cyber threats, asset compromise and physical, political & strategic risks

Silobreaker

www.silobreaker.com

A Terrifying Diagnosis: Cybercriminals Are Attacking Healthcare (But We Can Fight Back)

By Pieter Danhieux, Co-Founder and Chairman/CEO of Secure Code Warrior

Cyberattacks have become a way of life these days. People almost expect to hear news about some new vulnerability or breach that affects everything from banking to aviation, or devices as diverse as smartphones and traffic lights. Even our homes are no longer completely safe. Entire cities and towns are being attacked by criminals almost daily with hackers demanding millions in ransom to restore compromised critical services.

But one place where we could hopefully still feel safe was at the doctor's office or even in a hospital. People are at their most vulnerable when reaching out to a healthcare provider. Human decency would almost demand that the local clinicians be allowed to do their noble jobs in peace. Unfortunately, that is not happening. There seems to be little honor among today's cyber-thieves. In fact, healthcare could be the next "great" cybersecurity battleground, with hackers attacking the very machines that diagnose medical problems, provide treatments and sustain life.

Threats are getting more personal than ever before.

Attacks against the healthcare industry are not new. Cybercriminals already know the value that patient information, personal data, and financial records have in the underworld and on the dark web. That information can be used to steal money directly from patients, or as a launching point for secondary attacks such as phishing and other scams. It's no wonder then that many of the most devastating attacks lately have been aimed at healthcare. Anthem Healthcare had 80 million patient records stolen. Premera lost 11 million personal files. CareFirst's total was 1.1 million compromised records, and the list goes on and on.

As of right now, attacks made directly against medical devices seem rare. However, at least one report suggests that the problem might be much more widespread, with hospitals not reporting the intrusions, or employees untrained in cybersecurity simply not recognizing that an attack is taking place right in front of them. The ability to compromise medical devices in frightening ways, such as using malware to add fake tumors to CAT scans and MRI results, has been conclusively demonstrated by security researchers. It's not very much of a leap to think that attackers may already be doing the same or similar things to medical devices in the real world.

Healthcare is also uniquely vulnerable to cyberattacks thanks to its increasing reliance on devices within the Internet of Things (IoT), tiny sensors that are connected to the internet and which produce incredible volumes of information. For the most part, securing the information produced by those sensors, the channels they use to communicate, and even the sensors themselves, has been little more than an afterthought. The number of potential vulnerabilities that an attacker could exploit hiding within those IoT-dominated networks is likely almost limitless.

IoT in healthcare poses serious risks.

Services critical to patient care – which in some cases weren't even imagined 20 years ago – are breeding grounds for both IoT-based and other more traditional vulnerabilities. Electronic medical records, telemedicine, and mobile health were all seemingly waiting for the boost of information that IoT could provide. It's no wonder that the commitment to IoT in the healthcare sector is staggering. MarketResearch.com predicts that by next year, the IoT market in the healthcare sector will reach $117 billion, and continue expanding at a rate of 15% every year after that.

In that environment, skilled attackers can find plenty of vulnerabilities that can be used to exploit medical devices. IoT sensors embedded inside medical devices generally communicate and produce their data in one of two ways. Some gather data and then transmit all of their findings directly to the internet for analysis. Others use a form of distributed networking known as fog computing where the sensors themselves form a sort of mini-network, collectively deciding what data to share with a central repository or platform. That data can then be further processed or directly accessed by healthcare workers.

Further complicating cybersecurity matters within healthcare is the fact that the industry has never embraced. nor agreed upon, data handling standards, methods or protections. Historically the healthcare industry has been served by manufacturers that offered their own proprietary technologies for medical devices. Today this includes the embedded IoT sensors, the communication channels the devices use and the platform for analyzing the data after it's collected. This makes most hospital networks a hacker's dream, or at least a fine proving ground where they can exploit everything from security misconfigurations to insufficient transport layer protection. They can try anything from cross-site request forgeries to the classic XML injection attacks.

The counter-punch we need is right in front of us.

Despite the potentially catastrophic consequences of these vulnerabilities being exploited, there is something to remain optimistic about: these security bugs are not new, powerful back doors opened by criminal masterminds. They're so common that it is frustrating to keep seeing them, time and time again. Part of the reason they rear their ugly head is through the use of legacy systems that have gone unpatched despite fixes being available, but the other is once again related to the human factor. Developers are writing code at a cracking pace, and they're concentrating on a slick, functional final product… not security best practice.

There is simply too much software being built for AppSec specialists to be able to keep up, and we can't expect them to constantly save the day with these recurrent vulnerabilities. It is cheaper, more efficient and clearly much safer if these vulnerabilities are not introduced in the first place, and that means security teams and developers must go the extra mile to create a robust, end-to-end security culture.

What does a great security culture look like, exactly? Here are a few key elements:

- Developers are equipped with the tools and training they need to squash common bugs (and understand why it's so important to do so)
- Training is comprehensive, easily digested and plays to developer strengths
- The outcomes of the training are properly measured, with metrics and reporting (not just a tick-the-box and move on exercise)
- AppSec and developers start speaking the same language: after all, in a positive security culture, they're working to achieve similar goals.

The possibility for disaster is still enormous, and goes well beyond just having a patient's medical records stolen. Injecting fake tumors into a scan could devastate a person anxiously waiting to hear if they have cancer. And changing out medicines or altering treatment plans could actually kill them. But, it only takes one cybercriminal willing to cross that line for profit, and you can guarantee that it will happen. Perhaps the next ransomware scam won't encrypt a hospital's data, but instead, ruin the diagnoses for thousands of patients. Or perhaps an attacker will threaten to alter medicines unless they get paid, literally holding lives for ransom.

It's clear that we can no longer follow the "business as usual" approach when it comes to cybersecurity in healthcare. We can't rely on one or two specialists at healthcare organizations to fix every problem. Instead, we need security-aware developers working on healthcare apps and devices to recognize potential problems and fix them before they are deployed at facilities. And even healthcare workers could use basic cybersecurity training.

It's true that nothing is more important than your health. Within the healthcare industry, maintaining good cybersecurity fitness for the future will depend on facilitating better overall security awareness today. Without serious treatment, this is an issue that is only going to get worse.

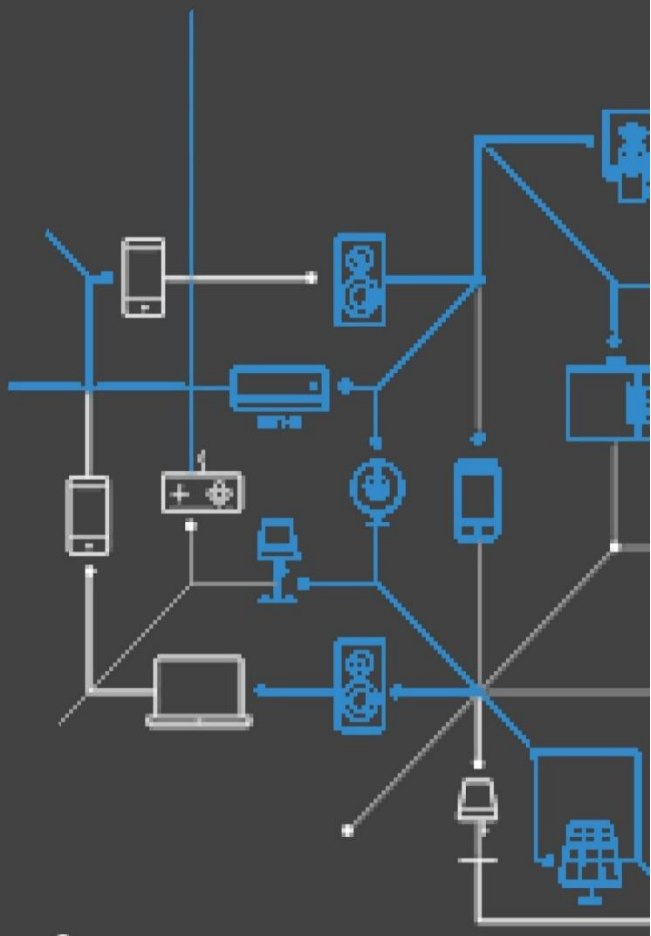
About the Author

Pieter Danhieux is a globally recognised security expert, with over 12 years' experience as a security consultant and 8 years as a Principal Instructor for SANS teaching offensive techniques on how to target and assess organisations, systems and individuals for security weaknesses. In 2016, he was recognised as one of the Coolest Tech people in Australia (Business Insider), awarded Cyber Security Professional of the Year (AISA - Australian Information Security Association) and holds GSE, CISSP, GCIH, GCFA, GSEC, GPEN, GWAPT, GCIA certifications.

Learn more about Pieter at https://insights.securecodewarrior.com/

SAM Protects Unmanaged Networks

85% of our customers are affected by DDoS attacks - SAM blocks all of them!



SAM's software only cybersecurity platform uses advanced fingerprinting to identify every device in a network and enforce enterprise grade security policies to protect users privacy and data.

Contact SAM for a live demo

www.securingsam.com

SAM

SEAMLESS NETWORK

Best Practices for Building A Comprehensive Cyber Risk Management Program

By Haythem Hammour, Product Marketing Manager, Brinqa

A primary goal for most information security organizations today is the identification, prioritization and remediation of cyber risk. Businesses struggle with risk management for a variety of reasons, including disconnected teams and stakeholders, limited resources, data overload and lack of consistency.

The enterprise IT infrastructure is evolving at a rapid pace. SaaS, IaaS, and cloud-native technologies have enabled businesses to embrace digital transformation, but they have also made enterprise IT environments more diverse and complex, and difficult to manage and secure. Software applications also represent an important attack surface. Most organizations' software infrastructure comprises very diverse entities – internally developed applications, externally sourced software, desktop applications, web applications, mobile applications, open source components, SaaS, APIs and web services.

The cybersecurity infrastructure to secure these elements is equally diverse. Different products may be used for testing for vulnerabilities in network, cloud, and container infrastructure. Separate, dedicated security products may be used for static application testing, dynamic or web application testing, and software composition analysis. Securing software infrastructure also requires DevSecOps, mobile security, penetration testing, and more. And, in most cases, these components and the corresponding security infrastructure are owned and managed by different teams, with little communication and collaboration.

A further challenge arises from the use of the cybersecurity tools themselves. They provide valuable and useful insights, but this data can easily get lost in a deluge of irrelevant information. Threat intelligence is a prime example of the need to identify and utilize relevant information while ignoring the noise. Making things more difficult is the reality that information about a particular entity may be distributed across multiple tools and locations.

Organizations need to be able to connect, model and analyze relevant security, context and threat data. That's the best way to deliver knowledge-driven insights for cyber risk prioritization, reporting and remediation. Companies need to implement a cyber risk management program that can:

- Intelligently connect vulnerability, asset and threat data from all sources for complete visibility and understanding of cyber risk.
- Prioritize remediation to address the most impactful, exploitable, and prevalent risks.
- Eliminate the noise of false positives and irrelevant information.
- Automate closed-loop remediation of risks at scale through creation, tracking and escalation of tickets.
- Narrow communication gaps across teams with a common data model, nomenclature, and language.
- Communicate real-time program metrics and risk indicators to all key stakeholders.

Information security organizations looking to build out their own cyber risk management programs should have the following best practice recommendations at the top of their minds:

Develop a comprehensive, extensible cybersecurity data ontology – Security teams must implement a cyber risk management process that is built on a comprehensive, standardized, and dynamic data ontology. Such an ontology will clearly define, delineate, and represent the common IT, security, and business components that comprise the enterprise technology infrastructure, and the relationships between them. To deliver risk insights that are relevant to a business, security teams must ensure that any unique organizational factors that have an impact on risk analysis are reflected in the cyber risk data ontology. The ontology must also be able to evolve with changes in the IT and cybersecurity landscape, without adversely impacting the risk management processes.

Expand the scope of cyber risk management to include network, applications, cloud, and emerging technologies – Organizations need comprehensive coverage of risk analysis and management across the entire enterprise technology infrastructure. InfoSec organizations must implement a consistent cyber risk management strategy across critical infrastructure components using dedicated, purpose-built processes for vulnerability management, network security, application security, cloud security, and emerging technologies such as IoT.

Adjust risk prioritization models as necessary – Another critical factor for success comes from being able to leverage information from disparate cybersecurity tools and stakeholders to develop and present new knowledge and insights in the form of risk scores, ratings, alerts and notifications. To do so, security teams need to have complete visibility and control over the risk methodology—resulting in accurate and relevant results and a better understanding of the factors driving risk prioritization and remediation.

Automate remediation management – Instead of ad hoc decisions, security teams should formulate and implement policies for risk remediation through automated ticket creation, tracking, and

validation. Strong, comprehensive capabilities around consolidation, dynamic ownership and SLA assignment can significantly improve the effectiveness of the remediation process.

Leverage cybersecurity process automation where possible – Cyber Risk Management involves processing and analyzing massive volumes of IT, security, and business data. This can be very time and resource intensive, and automation should be used where possible to alleviate these needs. Automated processes for risk analysis, prioritization and reporting not only make the program more efficient, but also lead to more consistent and accurate results.

Develop and communicate integrated analytics – For a cyber risk management program to function effectively, it must intuitively engage and inform all the varied stakeholders across IT, security, and business at the appropriate instant in the risk lifecycle. The ability to visually communicate key risk and performance indicators through powerful metrics and reports are crucial to program success. Organizations must empower and encourage stakeholders to develop and communicate the metrics and reports that matter to them.

The pace of change in enterprise IT is not letting up and cyber risk management programs must evolve and grow to keep pace. Best practices are taking shape as businesses and the public sector come to terms with the scale of the challenge. These include establishing and maintaining an extensible cybersecurity data ontology as well as process automation, integrated analytics, use of the open risk prioritization model and more. With such practices in place, the challenge of protecting complex enterprise software infrastructure becomes more manageable and dynamic.

About the Author

Haythem Hammour is Product Marketing Manager at Brinqa. A customer-focused Information Security professional and Cybersecurity evangelist, Haythem uses his engineering background and diverse experience to inform his work and to successfully collaborate with engineers and creative teams. Haythem is a Certified Network Defender (CND) and an official member of both the Product Marketing Alliance and the Forbes Communication Council. Learn more about Haythem at https://www.brinqa.com/

By the time an attacker tastes the difference, their presence is known.

"Attacker mistakes are made when they cannot distinguish real from fake."
Tony Cole, CTO Attivo Networks

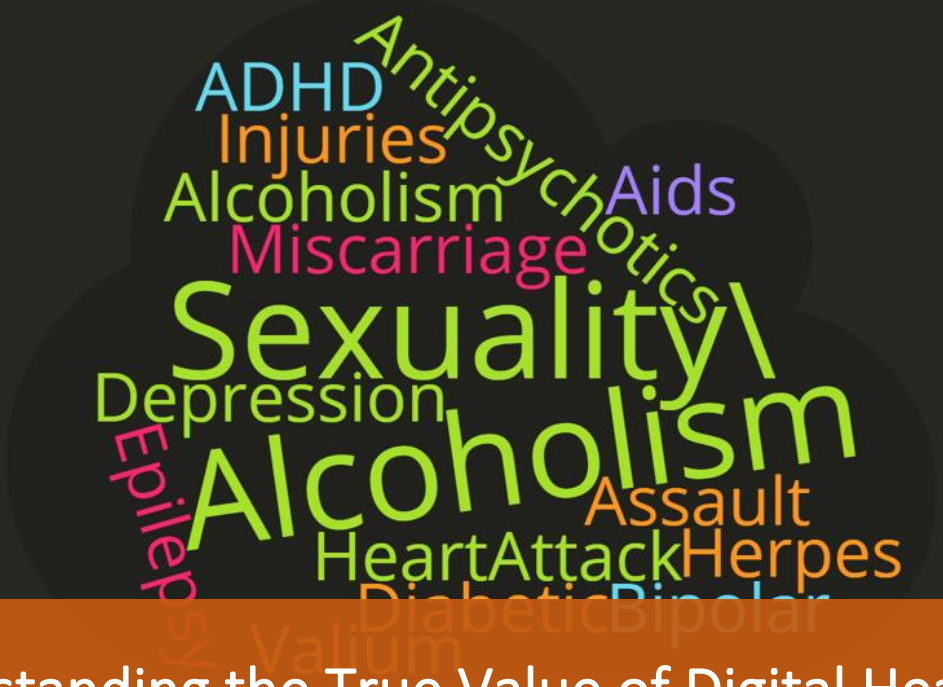
DECEPTION-BASED THREAT DETECTION

Detecting threats needs to be comprehensive, however it doesn't have to be complicated. Designed for simplicity, Attivo Networks brings uncertainty to the mind of the attacker, redirecting them away from the target assets and providing defenders with high-fidelity alerting that is backed with actionable attack and forensic data on malicious activity and insider policy violations.

Attivo NETWORKS®

Deceive. Detect. Defend.

Learn more at attivonetworks.com/ebook



Understanding the True Value of Digital Health Data

By Anne Genge, CEO and co-founder of Alexio Corporation

The story of Bob

'What do I care if someone reads my dental chart?" This is what Bob said before I broke it down for him. Bob didn't realize that when he filled out all the forms at his dentist, it included all the perfect details to re-create his identity. These details include not just regular contact details, but also his date of birth, his employer, insurance information, credit card details, email address, emergency contacts info, and then the scariest thing of all: his medication and previous health history.

Bob started to squirm as I asked him if it would be ok if I printed a few copies and posted them around the neighborhood, some at work, and at his kids school. Most people don't think about the fact that every single healthcare provider collects the most intimate details of our lives, and stores them in a computer. This computer is connected to the internet, and when hackers steal this information, they can do a lot with it. First, they leverage it themselves; next, they post it for sale on the dark web, so any other enterprising bad guys out there can attack you.

I gave Bob some examples of how his personal health data can be used:

- Compete Identity theft
- Mortgage Fraud
- Insurance Fraud
- Bank/Financial Fraud
- Extortion
- Cyber-attack on him and/or his??? in the future
- Public exposure of embarrassing details of his life

How much are you worth to hackers? Actually, you'd be surprised.

Some of the information you protect the most is worth the least on the dark web – for instance: a social security number is only worth 10 cents. A credit card number is only worth 25 cents.

What they DO want to get their hands on, however, is your electronic health record, which is a hacker's jackpot: it's worth hundreds or even thousands of dollars.

Where Does Your Health Data Reside?

Think about all the places you have provided your health data; do you know for sure that they're secure? Most people will automatically think of their doctor, their dentist, their physiotherapist. However, keep in mind that you share your personal health information far more widely than that:

- You disclosed your private health info to your life insurance company in order to get coverage, and may have even submitted to tests
- Your employer often has r-[0ecords of time off, whether for physical or mental health reasons
- Any specialist you've ever seen for any reason
- For your child: their school also has some limited health information
- Your local pharmacy (where you fulfill your prescriptions)
- Your health insurance company
- If you've ever called them, your employee assistance program will also retain some information
- The government

What Can Be Done?

Start by asking questions. We obviously need these services, so abstention is not necessarily an option.

What we need is to make sure that these different agencies and businesses ensure the privacy of our data and build that into their business planning.

Here are a few questions to ask them:

1. Do they store your data on a secure, monitored server?
2. Who has access to your data? Is that monitored?
3. Do they encrypt every email with your health or financial data in it?
4. Have they ever had a data breach?
5. How recently has the staff completed a cyber-security training program?
6. How often do they do updates to their security software?
7. Are their computers monitored for breaches?

These questions can tell you everything you need to know about the clinic or agency you're about to engage with.

Why should you care?

Health care information is as personal as it gets.

Our medical records contain the most sensitive and embarrassing details about us. Anything we've ever told our doctor, our medication lists, therapy notes, addictions, and mental health: these are just a few examples.

These details are not like a credit card number that can easily be changed. Steal our credit card information and what happens? Our bank has algorithms that detect unusual activity; they call us, suspend our card until they can get us another, and reverse the charges by the data thief. Doesn't sound terrible – inconvenient, at the most.

The Worst-Case Scenarios

Education is key in order to avoid these scenarios, but education on this topic is lacking, or is dependent on employers…where else does one learn about data security?

Many data breaches are a result of accidents: human error / mistakes – on the part of personnel in small practices. While they usually have your best interests at heart, small practices don't always prioritize data security, which means the personnel there aren't always up-to-date in their education, and to how to prevent breaches.

What You Can Do

Firstly, pay attention to articles that deal with data breaches – there are several that detail who's been hit, how many records have been compromised and to what level. Just like a recall on your car, this is information you should be monitoring in order to determine whether you need to be concerned or not.

Secondly, only give away the information you need to; don't volunteer health info – online or otherwise – unless you know it's from a trusted provider with (at at least a minimum of) basic security practices in place.

Why Health Data is So Important

The reason health data is prized above all others is because of how privileged it is. Most people don't want it broadcast that they have been treated for HPV, HIV, or any number of other conditions. However, this is exactly what hackers rely on – they know that we want to keep our secrets, and many people have had their privacy held hostage at the hands of unscrupulous characters.

If you've been nervous about the security of your healthcare records, join the club. Pass this article along to your healthcare providers to start an important conversation about cyber-security in health practices.

Get Alexio

If your dentist, physician or massage therapist doesn't yet have a cyber-security officer or plan, then it may be time to switch. However, if you love them as much as we love ours, you may want to simply pass them this article.

Alexio is a cyber-security company that's designed specifically for the healthcare industry, and helps them ensure privacy and data security for their patients using automation and machine-learning technologies. Education for the protection patient health information is also at the forefront and they deliver training to healthcare professionals as well as IT providers supporting them.

Alexio works with numerous other types of small businesses in order to ensure that everyone has access to enterprise-grade cyber-security, because it's too important to only be available to those with the biggest budgets.

If you're a small business, a healthcare practice owner, or a customer of any type, we're here to help. Learn more: getalexio.com I Listen to the podcast: https://youtu.be/vg81sNPl_NU

About the Author

Anne Genge is the CEO and co-founder of Alexio Corporation. Alexio is located inside the IBM Innovation Space, IBM Canada Headquarters in Toronto, Canada. She and her team of certified privacy and security professionals help dentists, physicians, and other healthcare providers to secure their data & systems, and comply with privacy laws & college mandates. She is a firm believer that good training in cyber-security is the key to protecting not just her family and clients, but also government bodies and major corporations. To this end, she has partnered with many organizations, including the Canadian Dental Association, and others to produce training in order to reduce the frequency of human error resulting in a security breach. Learn more about Anne https://getalexio.com/

TOP 10 ACTIVE DIRECTORY SECURITY BEST PRACTICES

1. Take regular backups and store copies offline to protect from ransomware and wiper attacks.

2. Always have sufficient backups to perform a full forest recovery.

3. Avoid bare-metal and system state restores when recovering from a malware attack.

4. Audit and alert on changes to critical / privileged group memberships.

5. Monitor for AD configuration changes that could indicate a DCShadow or similar attack.

6. Limit editing and linking of GPOs to a small subset of administrators.

7. Implement admin tiering to minimize credential theft.

8. Monitor for Kerberos-enabled service accounts with weak passwords to prevent "Kerberoasting" attacks.

9. Monitor for unconstrained delegation (and changes to delegation) on computer accounts.

10. Monitor for changes to the AdminSDHolder object to prevent administrative account takeover.

IDENTITY-DRIVEN CYBER RESILIENCE

Semperis is an enterprise identity protection company that helps organizations recover from cyber breaches and directory service failures, on-premises and in the cloud. Our patented technology for Active Directory is used by customers in the Fortune 500, government, financial, healthcare, and other industries worldwide. Semperis is accredited by Microsoft and recognized by Gartner.

SEMPERIS

Learn more at SEMPERIS.COM

Firewall Sandwich: A Hacker's Delight, Unless…

No single solution can offer a silver bullet for cybersecurity. Nevertheless, critical facilities such as manufacturing plants and power stations are currently in danger of relying too heavily on firewalls by regarding them not merely as a first line of defense, but as impenetrable barriers.

By Ofer Shaked, Co-Founder and CTO of SCADAfence

Recent Cyber-Attacks on Energy Grid Firewalls

Energy grid operations in California, Wyoming, and Utah were disrupted in March of this year by what is now believed to have been a Denial of Service (DoS) attack that exploited a known vulnerability in a firewall used by the facility in question. But even those firewalls that do not yet have known vulnerabilities, can only offer partial security for vital utilities such as power stations.

Ever since Russian cyber-attacks blacked-out parts of the Ukraine energy grid in 2015, power stations have been identified as soft targets by hacker groups now known to be sponsored by states such as Russia and China, as well as by organized cyber gangs demanding ransoms. No single line of defence can possibly provide full protection against state-level tactics, techniques, and procedures (TTPs).

The Security Challenges of Industry 4.0

In any case, the security perimeter is now expanding well beyond the boundaries of any firewall. As we enter the fourth industrial revolution, often referred to as 'Industry 4.0', power stations have little alternative but to accelerate the process of digitization that began when internet connections eroded the "air gap" security layer provided by the stand-alone systems traditionally used to operate energy facilities.

The process of digitization also frequently involves the use of third-party services and systems providing hackers with further ways to circumvent firewalls. The recent inclusion of previously stand-alone systems such as surveillance cameras and building management systems into the Internet of

Things (IoT) also creates further vulnerabilities in power stations, manufacturing facilities, and "smart buildings".

As those operating power facilities increasingly reach out to third-parties for new IT hardware and software and services, they open potential new doors for hackers. Any organization working closely with a power or manufacturing facility needs to be secured just as effectively as the systems running the power facility itself. Organized cyber criminals and state-sponsored hackers have become increasingly adept at using poorly-secured third-party systems to infiltrate otherwise secure organizations with malware.

Hackers Now See Firewalls Only as Temporary Obstacles

Firewalls on their own also do little to protect facilities against the greatest security flaw of all – human error. Hard-pressed software engineers working to tight deadlines, for instance, sometimes make configuration errors that can be identified and exploited by threat actors before they can be fixed. This type of error is hard to anticipate or detect as staff often try and cover up procedural mistakes. Staff using email are also increasingly prone to socially-engineered spear-phishing attacks that craft emails consisting of a brief message typically purporting to come from the facility's IT department or from a manager or senior executive.

With so many attack vectors at their disposal and with access to state-level TTPs, hackers now see firewalls as only temporary obstacles at most. Even the deployment of multiple firewalls, the so-called "firewall sandwich", represents little more than a series of speed bumps in the road to organized hacker groups determined to break into supposedly secure facilities.

The Effective Way to Safeguard Utilities

The only effective safeguard for utilities such as power stations is to monitor all activity on the facility's operational technology (OT) network. Ideally, passive technologies should be used to monitor activities within the OT network without affecting its efficiency in any way. To achieve this, a passive platform must be capable of catering for the very high outputs generated by the increased digitalization of OT in order to ensure minimal numbers of false positives.

SCADAfence connects to the OT network by using taps or port mirroring, basically providing a replica of the network's traffic for analysis, making it possible to identify indicators throughout the cyber kill chain in order to warn the security teams of a potential attack before it materializes. Pre-defined integration to other security controls, such as SIEMs and Firewalls, allows users to define automated actions for the response. The SCADAfence platform also allows users to investigate security incidents, control "logical" segmentation (identifying communications between two segments which should not be communicating), providing device-based risk management and many other useful tools that allow users to deal with effectively with cyber threats in OT environments.

About the Author

Ofer Shaked, Co-Founder and CTO of SCADAfence. Ofer Shaked spearheads technological initiatives that enable SCADAfence's products to support the ever-growing scale of the world's largest plants, and is in charge of SCADAfence's technological vision and innovation. He started his professional career in OT security in the IDF Intelligence elite cyber unit, where he accumulated vast hands-on experience. Since then, he has been advising key decision makers and leaders in the OT, Network and Security spaces, helping to plan secure corporate- and plant-level OT architectures.

Learn more about Ofer https://www.scadafence.com/

The Weakest Points in Your Network Are Your People

How to automate your network edge security to protect against human error and prevent cyberthreats from spreading

By Graham Walker, VP Marketing, Allied Telesis

"Protect your network borders; don't let the bad guys in!" is a persistent message coming from cybersecurity vendors. While this may be a prudent strategy, it's not the only one a modern organization should adopt to protect its network. Every week we see examples of network breaches, data theft, and cyber-crime affecting organizations of all sizes and across all industries.

The fact of the matter is that threats do not only come from malicious sources but also manifest themselves as accidental configuration errors by trusted network admins and from employees following poor security practices. Both ultimately lead to network outages, disrupting business through exploitation or neglect of these vulnerabilities.

A 2018 Cost of a Data Breach Study found that around 25% of all US data breaches resulted from carelessness or user error. It's time that companies realize that even if they have adopted conventional network security measures, their most significant vulnerability is their people.

There is no exception even to the largest organizations with abundant resources. In July 2019, Capital One Financial Corp. revealed it had discovered a breach affecting 106 million people in North America. Forensic analysis found that a configuration vulnerability had enabled a cyber-thief to download 30 GB of sensitive financial information. If a large financial services company like Capital One failed to get it right, what can we expect of everyone else? The correct assumption is that

companies must expect a security breach will eventually occur and urgently adopt a variety of strategies to plan for it.

Security that isn't secure

It's incredibly challenging to build a network that has a 100% secure border. Almost all networks have vulnerabilities, and often, the people that work within the network offer the highest risk. Yet, very few companies adequately train their staff with the necessary skills to identify and prevent these threats. MediaPro's State of Privacy and Security Awareness report claims that 70% of US employees don't understand cybersecurity.

Sometimes breaches are deliberate and malicious, where an employee abuses their trust and causes damage, steals, or facilitates others to steal from the company. Restricting access to sensitive data, data leak prevention, network segmentation, enforced policies and procedures, and audit trails are effective ways to limit this exposure. Although insider threats are less common than external threats, the damage can be worse, and a determined actor with malicious intent and access to company data can be almost impossible to stop.

One of the most infamous and damaging insider breaches was when the contract employee Edward Snowden stole classified information from the National Security Agency (NSA) and exposed it to journalists. If one of the top security-conscious agencies on the planet can't safeguard and prevent its most confidential secrets from insider threats, what other organization out there can?

A more common threat is the inadvertent mistake of an employee who "just forgot" or "wasn't thinking". According to the Ponemon Institute Cost of Insider Threats Report, 65% of insider incidents in 2018 resulted from accidental mistakes or misuse. These common mistakes often include the use of unknown USB sticks, sharing passwords (yes, this still happens), storing sensitive information on unsecured devices then losing them, connecting unauthorized devices to the company network, falling prey to phishing campaigns, forgetting to apply a security patch, and more. Each of these mishaps has the potential to invite a multitude of threats that may lead to business disruption, reputational damage, significant fines, and other financial outlays.

Consider the class of mistakes that enable threats to enter the network by a backdoor or an alternate route other than the usual email or weaponized website. Since most organizations rely on their firewall to protect them from threats—the "secure border" model - these mistakes are of critical concern. Bypassing the border (just as the Greeks entered Troy inside the famous wooden horse!), leaves the network defenseless, and allows threats to spread and wreak havoc with nothing to stop them.

Even worse, in the event of the firewall telling the administrator that it sees a threat, what can the admin do about it apart from pulling network cables out? These threats can spread too fast for a human to react. Hence it is a justified approach to defend the border at all costs and keep the bad actors out—the reason being that once the attackers get inside, as the Trojans discovered, it doesn't end well.

A solution you can rely on

The better approach is to apply a different, forward-thinking strategy that accepts threats can and will enter the network but offers solutions for how to deal with them effectively and rapidly. Ideally, the network itself would not only identify the threat but also take immediate action to shut it down

and quarantine any affected devices before more damage is done. This is precisely what the Self-Defending Network solution from Allied Telesis does.

No replacement or reconfiguration is required for the existing firewall as the Self-Defending Network can react whenever the firewall sees a threat to identify the source and isolate the affected user device. Other solutions do the same thing, but they all require agent software to control the endpoint devices. This complicates the deployment of new devices, adding to the administrator's busy workload and limiting the solution's value.

Our Self-Defending Network is different because we control the network and not the device. There is no agent software to deploy, and we can protect against threats on any user device, including mobile, since we can control both wired and wireless networks. However, the primary advantage is that the responses to threats are immediate and automated. So, a threat can be shut down quickly and without manual intervention, giving it no chance to spread, therefore solving the problem of how to stop a threat from spiraling out of control once it penetrates past the border. As this solution is automated, the risk of human errors is vastly reduced, particularly useful in a crisis when stress levels are high.

The Self-Defending Network is built on our automation engine, called Autonomous Management Framework (AMF). AMF contains an intelligent security component called AMF Security (AMF Sec), which works with threat detection applications to instantaneously respond to alerts and block attacks within a wired or wireless network. Unlike other solutions that control the endpoint device, AMF-Sec isolates and quarantines compromised endpoints without the need to install agent software.

When a threat is detected, AMF-Sec responds to locate and quarantine the suspect device immediately, without affecting other network users. Responses are configurable – for example, log a message, block the device, quarantine it on a VLAN – and comprehensive logging provides a clear audit trail on what has taken place. Remediation then can be applied by the network administrator so the device can re-join the network with little to no disruption.

Deployment is painless because AMF-Sec works with a wide range of physical and virtual firewall products without any reconfiguration. Two options are available for communication with network switches: either with OpenFlow or AMF. AMF-Sec can use either method to control device access, which provides flexibility and reduces the need for equipment changes.

The takeaway is this: The Self-Defending Network works with your existing firewall to deliver real value with immediate threat responses and reduced operating costs without increased complexity.

Conclusion

The conventional security approach concentrates on defending the network border, working on the assumption that it is the only way threats can enter the network. As we have shown, this is not true, and companies that adopt this approach can be blindsided if they do suffer an insider attack. Whether the attack is malicious or the result of human error, the consequences can be devastating. Therefore, organizations must be well-prepared for insider threats in whatever form they take.

The most effective countermeasures are frequent security awareness training and implementing best practices such as least-privilege, need-to-know, network segmentation, etc. However, it's wise to adopt a belt-and-braces approach that reinforces best practices with automated solutions to reduce mistakes and defeat malicious actions as soon as they are detected.

About the Author

Graham Walker is the Vice President of Marketing for Allied Telesis. He has worked with Allied Telesis for almost 20 years, having recently moved to the US from Allied Telesis Labs in New Zealand where he was the Product Marketing Manager for the APAC region.

Graham's experience includes software development, project management, and product marketing. He is a forward-thinking professional who enjoys understanding customer's requirements and discussing the benefits and pitfalls of technology. His focus is to ensure that everyone knows that Allied Telesis make secure and reliable networking easy!

Graham holds a bachelor's degree of Computer Science from Strathclyde University in Scotland and can be reached online at LinkedIn and via our company website https://www.alliedtelesis.com/

The Evolution of Cybersecurity In 2020

Why security is moving from the IT department to the boardroom

By Chad Walter, VP of Sales and Marketing, IGI

Cybersecurity experts are constantly looking to the future to predict trends in the industry and anticipate new technologies. We are all hearing the buzz around how technology at the IT level is the answer, which has spawned the chatter around Artificial Intelligence, Machine Learning, and Unified Threat Management—but the most prominent trends for the year ahead might be simpler than that.

The most prominent change in the cybersecurity landscape is that it's become part of the core fabric of businesses, moving the security discussion from the IT department to the boardroom. It's no longer sequestered to the back burner of IT admins, and no longer just the responsibility of the security and compliance officer who is nothing more than a scapegoat or compliance checkbox. More and more, cybersecurity consultants are speaking directly to the strategic decision makers such as the CEO, President, or even the Board of Directors, and the CISO (Chief Information Security Officer) has joined the business strategy team as an influential stakeholder.

In fact, IGI has recently been involved in several cybersecurity engagements where our client's sales function was the driving factor for the cybersecurity services decision. Many of our clients found themselves having to prove their cybersecurity posture in order to land multi-million-dollar contracts. In other cases, merger and acquisition activity was driving the cybersecurity conversation. These are just two examples of when the cybersecurity decision wasn't about a technology or some compliance requirement, but rather were driven by core business success, or for that matter potentially losing key clients.

Another example of this trend is when IGI was introduced to a manufacturer who, by all practical purposes, didn't have serious compliance requirements or mandates and their exposure to risk was very minimal. They have 2000+/- employees (Yes, they need to protect employee data, but companies have historically ignored this critical piece),there are no proprietary technology secrets to protect, and they don't take credit cards. They do produce a product we all rely on, but it's not at

all critical. When asked, “Why do you invest in cybersecurity?”, the answer perfectly reflected the shift in mindset that we’re seeing.

“We invest in cybersecurity because we have a responsibility to our employees.”

The customer went on to say that they treat their cybersecurity investment as a benefit to employees. For example, when they conduct security awareness training programs, they are investing in education for their employees, which also includes life skills that they can use both at work and at home. This may be a unique approach, but it’s slowly becoming more prominent among companies of all sizes and in a variety of industries. It’s not just about checking a box or meeting an IT requirement, more and more cybersecurity is instrumental in the overall success of a company.

We know that cybersecurity is harder today than it was a decade ago. It may not take a village, but it does take a very specialized team to manage cybersecurity successfully. There are no silver bullets and there is no one “super-person” you can hire to completely manage every aspect of your security posture. Expecting any one person to handle all your cybersecurity requirements is like drafting a quarterback to win the championship by themselves. Like football, cybersecurity takes an entire purpose-built team. IGI takes on that quarterback role, calling plays and driving down the field, but is backed by an entire team to do the heavy lifting.

Despite advancements in cybersecurity technology, (and in some cases, because of cybersecurity technology) cybersecurity continues to grow in complexity. This challenge coupled with the massive cybersecurity talent shortage means that even when companies can find the talent, they can’t afford it, they may not require the talent full-time, or they can’t find *enough* resources to meet the needs of the organization.

Building on what we experienced throughout 2019, companies will continue to look externally for the true cybersecurity focus that they require in 2020. Companies will seek partners like IGI to address key pain points and anticipate the needs of their organization. Our core services include Virtual CISO, Managed Detection & Response (MDR), Penetration Testing, Incident Response, and Vulnerability Management—and can all be part of a strategic, managed program that aligns with your business strategy.

Your Cybersecurity Team must understand both the cybersecurity landscape, as well as your business initiatives and strategy to fully manage and protect your infrastructure.

Learn more about how IGI’s purpose-built team can help your organization at https://www.igius.com.

About the Author

Chad Walter is the VP of Sales & Marketing at IGI cybersecurity. Chad has spent 14 years in various roles in the cybersecurity industry and currently leads the sales and marketing teams at IGI. Chad can be reached online at cwalter@igius.com on LinkedIn at Chad Walter and at our company website at https://www.igius.com.

DATALOCKER®
SIMPLY SECURE

Please visit us at
North Expo 4419

For unmatched simplicity and ultimate security,

trust SAFECONSOLE®

*to control, inventory, **audit** and **manage***
*your **DataLocker** encrypted endpoints.*

PortBlocker
Managed USB Port Control

SAFECRYPT
Managed Encrypted Virtual Drive

Vulnerability Management Democratized

New solutions are built with ease of use and efficiency in mind

By Todd Nielsen, Director, Product Management, IGI

Vulnerability Management has always been complicated; it required pro tools (read, expensive), time consuming workflows (read, expensive), and sophisticated training for users (read, expensive). It used to be the sole domain of cybersecurity experts with a deep understanding of all the vulnerabilities that adversaries exploit. Those days are over.

Cybersecurity, including vulnerability management, can be complex and overwhelming. The reality is that not all security solutions are designed for simplicity—some do what they're designed to do very well and are not built with ease of use in mind. But when it comes to VM, there's no reason it shouldn't be straightforward.

From a 30,000-foot vantage point, the VM landscape is simple. Vulnerabilities are the entry point that adversaries exploit in most breaches, which isn't surprising since our networks change every minute. The devices, configurations, operating systems, and applications are all highly dynamic.

VM solutions illuminate your entire network inventory, identifying (or 'fingerprinting') each device and enumerating all known vulnerabilities. With a VM solution in place, the organization has visibility into network vulnerabilities and the knowledge to prevent cyber incidents.

Finding vulnerabilities is the first step in a holistic Vulnerability Management Strategy ("VMS"). VM software is a critical component, and only impactful as a prevention strategy when it includes asset discovery, identification of vulnerabilities, and prioritized remediation workflows to close the gaps. From that vantage point, VM is a cornerstone for any cybersecurity program. Yet, it's often the overlooked element of a complete cybersecurity program and typically viewed as overcomplicated, time consuming, and expensive.

That's what inspired Nodeware®: efficient by design and made for everyone. Nodeware, built by IGI, was created by cybersecurity experts and for cybersecurity experts. The IGI team has the advantage of understanding the cybersecurity industry on a deep level and is therefore in a unique position to develop innovate, purpose-built security products like Nodeware.

Nodeware is a powerful VM solution that also delivers on the promise of powering a VMS that does not require a team of credentialed cybersecurity experts. Nodeware was built for cybersecurity consultants who were bogged down by cumbersome, complicated, and *expensive* vulnerability management tools.

As a purpose-built solution designed to be powerful enough for cybersecurity experts, Nodeware differentiates itself in the market with fast, intuitive setup and simplified management that every IT professional can understand. It's ideal for the channel market because it does not require cybersecurity expertise or extensive training, which is why Nodeware users include MSPs, MSSPs, VARS, and internal IT departments.

Nodeware is extremely effective in device management and vulnerability scanning because it never sleeps, taking persistent inventory of the network all while using virtually no network resources (less than 5% network utilization). Leveraging multiple databases tracking more than 128,000 known Common Vulnerabilities and Exposures (CVEs), Nodeware uses real-time vulnerability scoring to target and prioritize vulnerabilities. Device and critical vulnerability information is displayed in real time on an intuitive dashboard, allowing MSPs and clients to see security gaps in real time. Nodeware's dashboard, alerts, and simple network scoring lights the path to more secure networks and a safer future. The unparalleled visibility into the network makes Nodeware a powerful tool to drive a successful VMS—no cybersecurity experts required.

In the channel market, Nodeware fills a hole in the SME space, which is an often-overlooked market segment in cybersecurity and vulnerability management. Nodeware is affordable and priced for the channel, at only a fraction of the time and money that other VM solutions ask of you. Designed around a recurring revenue model (monthly SaaS subscription), Nodeware has the added bonus of driving revenue through additional services, such as remediating vulnerabilities.

Nodeware also integrates with tools you use every day, helping to bring cybersecurity into your daily workflows via Slack, Zapier, Microsoft BI, and more.

Nodeware is made for MSPs, MSSPs and VARs seeking an edge in their portfolio, and the advantage of delivering superior cybersecurity to their clients. For non-security focused MSPs, it serves as the elegantly simple, efficient solution to drive a cybersecurity business—no cybersecurity credentials required.

Learn more at www.nodeware.com.

About the Author

Todd Nielsen is the Senior Product Manager at IGI, the cybersecurity company that developed Nodeware vulnerability management. He leads the development of IGI's Security Services, Managed Detection & Response, and Nodeware Vulnerability Management software solution. Todd is focused on achieving, optimizing and maintaining peak customer experience, as well as managing product roadmaps that navigate our offerings through the intrepid landscape of cybersecurity, on the march to safer futures.Todd can be reached online at tnielsen@igius.com, on LinkedIn at and at our company website at https://www.igius.com.

Do you know who's on your network?

We do!

Not all devices are visible. It is important that you see **ALL** devices in your environment to exercise granular control to mitigate risks and data loss.

The WootCloud HyperContext™ Device Security Platform

- Discovers ALL devices on multiple spectra — Network & RF
- Profiles EACH device analyzing 300+ parameters
- Sanctions EVERY device automatically and at scale

HOW IT WORKS

Installation
- Campus
- Branches

Coverage
- Network devices
- RF devices

Data Collection
- WootCloud sensor
- IPFIX/Span port

HyperContext
- Device context
- Network data
- Threat intel

Remediation
- Policy based
- ML engine tweaks

WootCloud HYPERCONTEXT

Call **1-888-4WOOTCLOUD** or visit **www.wootcloud.com**

World's Largest Cybersecurity Unicorn Lives in China

By Edward Tsai - Director of Investment, Qi An Xin

Who would think that the world's largest Cybersecurity unicorn lives in China? In China, everything is at a larger scale. As of September 2019, China had 1.6B mobile phone subscriptions and by the end of this year, China will be over 55% of global online retail sales. Within China's rapid digital transformation and the maturing of the consumer tech ecosystem giants, Chinese entrepreneurs, investors, and the government have begun to focus on core technology and enterprise-related sectors such as AI, Semiconductors and Cybersecurity. Cybersecurity policy enactment through the 2017 China Cybersecurity Law in addition to the digital transformation priority of Chinese enterprises and government entities has led to an increase in Cybersecurity spend to over 50B RMB in China in 2018.

Within Cybersecurity, Qi An Xin has emerged to be the leading Unicorn not only in China, but also in the world. In July 2019 report by CB Insights on global Cybersecurity unicorns, Qi An Xin had the largest disclosed total funding and the second highest valuation in the world.

Vision

A company's fundraising strategy is reflective of its overall strategy. As the Chairman of Qi An Xin Group, Xiangdong Qi has already had prior success in Cybersecurity, having co-founded Qihoo 360 which prior to its privatization was a $9B USD market cap company on the NYSE. Qihoo 360 had already become the largest consumer Cybersecurity company in China, with ~500M PC users of its Anti-virus software, and over 4000 employees. This prior experience was the beginning for Xiangdong's long term goal of creating the world's largest Cybersecurity company.

Becoming a Unicorn

In order to do this, in the middle of 2016, Xiangdong led a management buy-out to spun out Qi An Xin from 360, focusing on the Enterprise Cybersecurity market. In 2017, Xiangdong raised Qi An Xin's Series A of 1.6B RMB at a 11.6B RMB post-valuation. To do this, Qi An Xin established a competitive fundraising process, collecting multiple Term sheets representing an an oversubscribed

amount of interest early on in order to hasten the process to final signing. Significant time was spent to educate investors on the Cybersecurity landscape in the US and China, and help funds see that Cybersecurity in China was a promising place to invest.

The earliest supporters of Qi An Xin's fundraise were a combination of funds familiar with the Qi An Xin team and other well-known investment funds who placed importance on national technology priorities. These included VC funds like AlphaX Partners as well as funds in large investment management groups like SDIC and CICC. At the close of 2017, Qi An Xin raised a 1.25B RMB round, this time from a Beijing Xi Cheng District affiliated fund, IDG China, and others, in total raising 2.85B RMB in its first full year as an independent company.

Qi An Xin's revenues grew from under 700M RMB in 2016 to nearly 2.4B RMB in 2018, becoming one of the fastest growing Cybersecurity companies in China. Qi An Xin's main product lines of endpoint security, network security, and big data security enabled it to have a large TAM and thus a massive growth and market opportunity. Through R&D and acquisitions, Qi An Xin also offered solutions in emerging areas such as threat intelligence security, industrial security and virtualization security. Qi An Xin's focus on utilizing big data analysis, enhanced by its large customer base in China, enabled it to offer its users more effective means to respond to security threats.

This growth enabled Qi An Xin to continue to successfully fundraise, raising 2.15B RMB in 2018 and 1.5B RMB in 2019, with a post-valuation of 23B RMB. In total, Qi An Xin has raised 6.5B RMB in funding to grow the company to now over 7000 employees. Over 40% of Qi An Xin's employees work in R&D, making Qi An Xin one of the largest employers of Cybersecurity R&D talent in the world.

Strategic Cooperation and Ecosystem

Earlier in 2019, China Electronics Company (CEC) acquired a sizable minority position of Qi An Xin and is its second largest shareholder. Together with CEC, Qi An Xin co-hosts the leading Cybersecurity conference in China, Beijing Cyber Security Conference (BCS). BCS enables Qi An Xin to help develop China's Cybersecurity ecosystem particularly covering new Cybersecurity technology, policy, innovation, talent development, and venture capital investment. In 2019, BCS hosted over 160 guest speakers, 500 companies, and was visited over 30,000 times. BCS is the host of the BCS "Innovation Sandbox" which is China's leading Cybersecurity startup competition, which has hosted 4 competitions to date and whose

participants have collectively raised more than 1B RMB in funding. Guanchao Cyber Forum is also a highlight of BCS, which runs sessions on international dialogue and collaboration in Cybersecurity policy.

As technology platforms develop globally, Qi An Xin has also developed international partnerships, including with VMWare on Cloud Security solutions and with Cyberbit on Cyber training. Qi An Xin also has international business in Indonesia, Singapore and Canada.

Future Growth

Qi An Xin continues to invest in Cybersecurity, recently focusing on "Security Built-In DNA", tightly integrating IT system, operations, and talent with Cybersecurity to create secure solutions and

continues to partner with other ecosystem players to make the internet a more secure place and the world a better place.

About the Author

Edward Tsai is Director of Investment at Qi An Xin where he leads a team responsible for fundraising, M&A, and investments. He prior was Assistant GM at Security Capital. Prior to this he was Director of International Investments and Director of Strategic Development at Qihoo 360, where he invested in AI and Cybersecurity companies and funds such as Life360, Cruise Automation, Brave Software and 1011 Ventures. Prior to moving to China, he was VP at DCM and Senior Associate Consultant at Bain and Company. Edward is a Kauffman Fellow (Class 15) and has a BS and MS in Computer Science from UCLA. Learn more about Edward https://www.qianxin.com/en

IGI

Solve.

Simplify.

Secure.

- VIRTUAL CISO
- INCIDENT RESPONSE
- PENETRATION TESTING
- SECURITY ASSESSMENT
- VULNERABILITY MANAGEMENT
- COMPLIANCE READINESS
- MANAGED DETECTION & RESPONSE

Learn more at
igius.com

Moving Network Security to The Cloud

What is secure access service edge (sase) and why it matters

By Paul Martini, CEO, iboss

The world of technology that exists today is substantially different from that of only a few years ago. The cloud has changed everything. Mobile phones and devices have allowed users to work from virtually anywhere. Applications which were once hosted within datacenters have moved to the cloud. The combination of mobility combined with business applications available in the cloud, from any location, has allowed companies to become more agile and productive. Bandwidth is through the roof and secure encrypted network connections are mandatory. While the revolution driven by SaaS applications provides new possibilities, the challenges they bring to the world of network security are substantial.

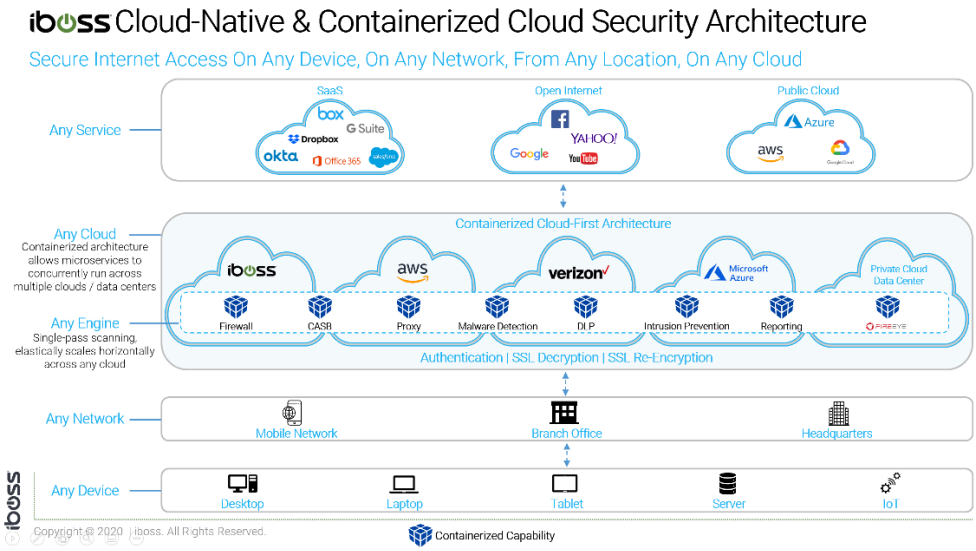
Network security is an area responsible for inspecting content as it moves between devices and the cloud. Fundamentally, network security technology stacks require access to the data in motion to prevent malware, detect breaches and prevent data loss. Traditionally, access to this data was very straight forward. Users were constrained to physical network perimeters, such as an office building. As devices interacted with public cloud services, the data could be forced through on-prem firewall and proxy network security appliances. The data was forced to flow through chokepoints before heading to and from the internet. With mobility, users are no longer constrained to any physical location. The data leaving their devices run on public networks and organizations do not have the luxury of forcing that traffic through company owned firewalls and proxies.

The data could be hair-pinned back through centralized datacenters before heading out to the internet but increasing bandwidth and the need for speed quickly makes this approach unsustainable and cost prohibitive.

Mobility changes the perspective of what the perimeter is defined by and completely inverts the traditional network topology model. Instead of using a physical building to define a network perimeter,

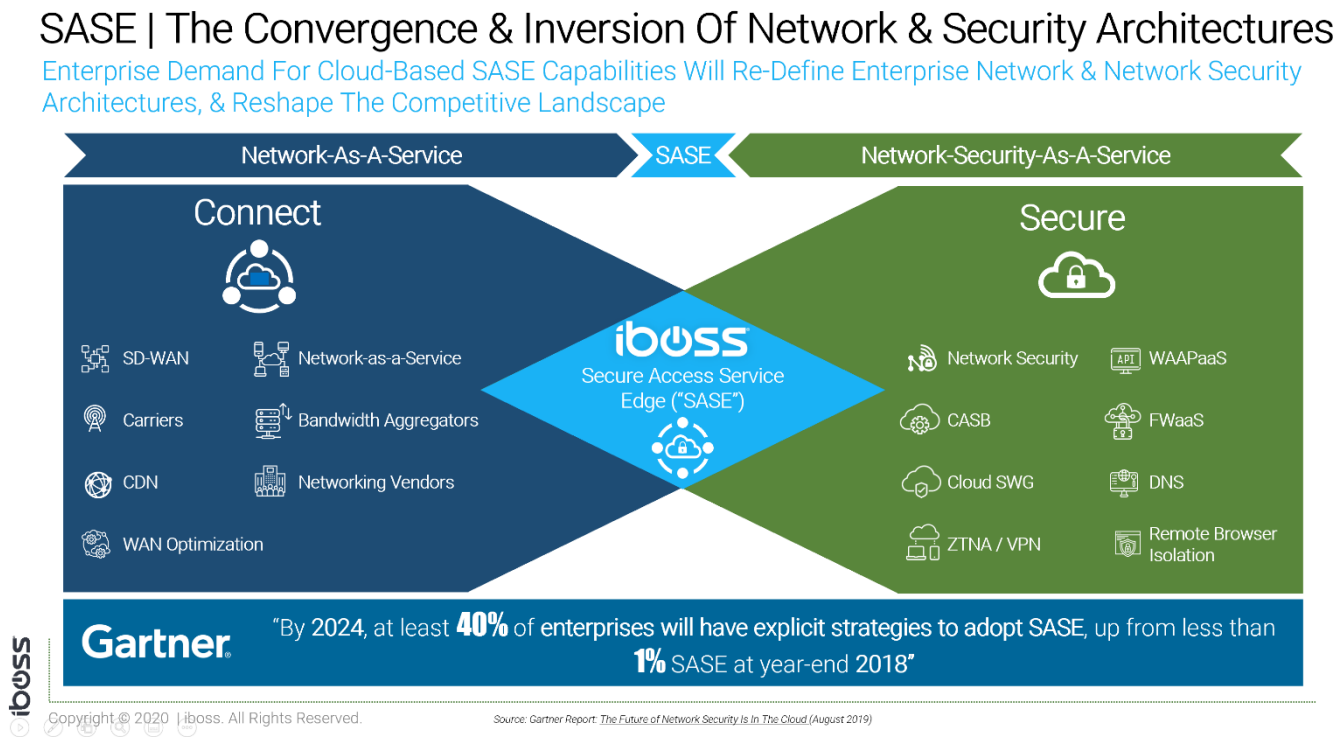
the device itself becomes the perimeter. A user working on the road is a network of one. A group of three users working from a conference is a network of three, essentially forming a remote branch office. The same could be said for branch offices or headquarters. The device and the user is where the network is defined and where trust should begin and end. Firewall and proxy appliances inherently do not fit this model because they are physical infrastructure designed to protect physical locations by inspecting all of the data leaving that location. In the new model, where should the firewall or proxy be installed? If a user is working from home, should a company owned firewall appliance be installed at user's home office? How will this help when the user decides to take their laptop and work from the road, immediately leaving the home network perimeter?

The network security functions are still required for both security and compliance. Intrusion prevention and inspection of network content for malware and data loss are fundamental techniques that are still required and essential. However, sending network data to appliances hosted at any specific location does not make sense when the connectivity is not originating from any specific location. This is where the shift of network security from on-prem network security appliances to network security delivered in the cloud is essential. Instead of sending device and user data to the network security appliance hosted at the datacenter, network security delivered in the cloud allows cybersecurity functions to move to where the user is located automatically. Since users are connected to cloud applications and cloud-based network security lives in the cloud as well, network security running in the cloud can move to the location from which those connections are originating. The network security functions in essence live where the applications live, in the cloud, allowing all data to be secured from anywhere.



To make things worse for an appliance-based approach to network security, the shear increases of bandwidth and encrypted data has been explosive. Network security appliances have theoretical throughput limits, governing the amount of data they can process and secure before becoming completely saturated and slowing down connections. Slow connections are just as bad as down connections because they drastically affect user productivity due to the inability to access business cloud applications efficiently. Network security delivered in the cloud is free from these restrictions as the compute and processing power available is not limited by any physical constraint and can scale on demand as needed. Cloud-based network security can decrypt any volume of content and inspect it for malicious or harmful transfers with ease. Containerized approaches to cloud network security also allow for low latency and fast connections with the ability to take advantage of horizontal scaling to process any volume of traffic.

Moving network security to the cloud is a requirement with the new reality of an inverted network perimeter that exists today. When evaluating cloud-based network security platforms, it's critical that the platform is able to deliver the same functionality found in network firewalls and proxies leaving only the appliances behind. Containerized architectures, like that found in platforms like iboss, allow both stream-based security functions found in firewalls and file-based security functions found in proxies to be delivered via a SaaS solution in the cloud. Containerization allows for raw packet processing capabilities which are required for firewall functionality, such as Intrusion Prevention protection. Ensuring that the cloud-based platform also has the policy engine capable of transitioning the network security functions mired in appliances to the cloud-based solution should also be considered.



In the Gartner paper titled "The Future of Network Security is in the Cloud" which introduced the SASE ("sassy") model which describes this new phenomenon which must be addressed for a sustainable path to the future. Cloud SaaS network security platforms, such as iboss, allow organizations to easily migrate from traditional on-prem appliances to a sustainable cloud-based solution.

About the Author

Paul Martini is the CEO, co-founder and chief architect of iboss, where he pioneered the award-winning iboss platform. Prior to founding iboss, Paul developed a wide-variety of complex security and technology solutions for clients such as Phogenix, the U.S. Navy, and Hewlett Packard. He was also a key contributor at Copper Mountain Networks working on designing and implementing FPGAs and broadband network infrastructure used by Telcos to build the cloud. His work at Science Applications International Corporation (SAIC) involved building distributed real-time systems for companies such as Rolls Royce. Copper Mountain and SAIC both launched successful IPOs. Paul has been recognized for his leadership and innovation, receiving the Ernst & Young Entrepreneur of The Year award and being named one of Goldman Sachs' 100 Most Intriguing Entrepreneurs. Paul holds over 100 issued patents in cybersecurity, networking and technology and has had his work published in many scientific journals, including the Journal of Foundations in Computer Science and the Journal of Analytical Biochemistry. He holds a Computer Science Degree from the University of California.

Paul can be reached online via LinkedIn at https://www.linkedin.com/in/martinipaul. For more information, visit the iboss company website at https://www.iboss.com.

VULNERABILITY MANAGEMENT

DEVELOPED BY

IGI

Identify your greatest risks and weaknesses before malicious outsiders can take advantage of them.

DISCOVER

Complete visibility of all assets, including IoT devices

FINGERPRINT

Identification of operating systems and services

SCAN

Expose weaknesses and gaps in your network

REMEDIATE

Fix critical issues & validate your security posture

Learn more at **nodeware.com**

Cyber Prevention Is No Panacea

Detection is Key When Prevention Fails

By Tony Cole, CTO, Attivo Networks

Last year Gartner estimated cybersecurity spending to grow to $124 Billion US dollars globally, and by 2021 to be over $170 Billion yet we consistently hear about major compromise after major compromise. What's going on? Why isn't the massive amount of dollars being pumped into our security infrastructure, paying dividends by stopping breaches?

It's really a simple answer: we're spending almost all of it on preventative technology, which doesn't always work to stop attacks. Today, battle-hardened security experts understand that we cannot prevent all attacks from getting into our enterprise and that we need to even the odds. We must allocate portions of our resources into quickly detecting attacks that overcome or bypass our preventative security stack. They understand that a determined attacker, given enough time and resources, can almost always find a way to get through our defenses. Our job isn't to prevent every attack since that isn't possible. It's to stop what we reasonably can and quickly detect any breach and promptly mitigate the impact of that compromise. In 2020, that's a win.

So how do we do it? Deception is how. There's a reason NIST has incorporated deception into multiple guidelines for industry and government such as 800-160, 800-53, and 800-171B. There's a reason that Gartner recommends deception since they state "simple, inexpensive, and it works," "we don't know any other technology that has a better signal to noise ratio," and "deception is the first starting point for detection." Deception's time is here so that we can detect threats inside our network quickly and accurately, allowing us to shrink breakout time, dwell time, and containment time.

So, what is deception? Modern deception platforms provide great capabilities in detection by minimizing lateral movement, detecting MITM attacks, protecting AD, providing analyst visibility, and much more. It puts the control firmly in the hands of the defender by locking down endpoints with deception and leading the attacker into an authentic decoy environment, using real operating systems, where you can track and study their malicious activity. This is done by installing dynamic and authentic-looking deception credentials on endpoints or into cloud environments, all leading adversaries into the authentic-looking decoy environment. You can further enhance this deceptive environment with deceptive mapped shares, which when touched, generate high fidelity alerts. If an adversary begins with AD queries, the deception module can hide the real credentials and return misleading AD information to the attackers, once again putting the defenders in complete control inside their own enterprise. When attackers attempt to move laterally, they are moving throughout the decoy environment, which tracks and monitors their activity, either for quick expulsion or to study their TTPs. Proper deception platforms can also work in almost any type of enterprise environment:

cloud, ICS/SCADA, and IoT. Some of those can't provide sufficient logging making deception critically important in providing new visibility in an area previously blind to cyber defenders.

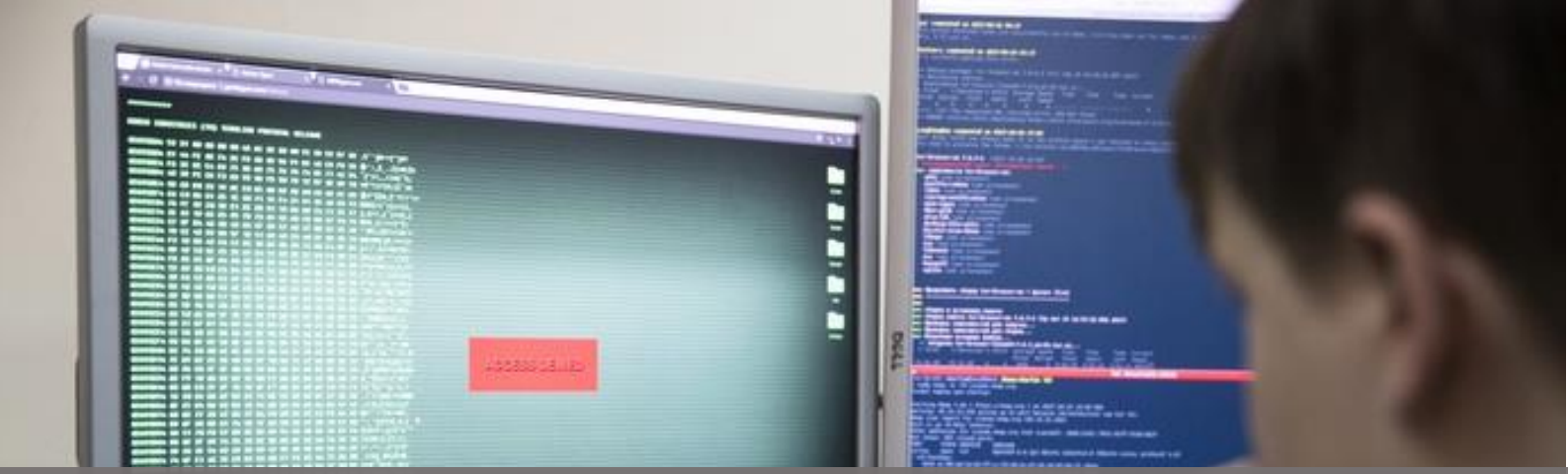
Deception platforms can be diverse and also limited in capabilities. Ensure you select one that can align to your goals, the campaigns you want to create, and that can look like your environment, whether that's an on-premises enterprise, in the cloud, a hybrid system, an IoT-heavy system or a utility providing power. It shouldn't matter; it must look like your system to be successful since authenticity is vital.

Our job is to protect our enterprise and minimize risk. To be successful in that endeavor, we must recognize that we cannot stop all attacks and, therefore, must have the instrumentation inside our enterprise to detect the attacker once they crossed the preventative security stack. EMA conducted a survey in 2019 where deception users saw on average a 91% reduction in dwell time. It's clear that deception is that answer to that essential requirement inside the enterprise, that it is, after all, the solution for detection. Early detection of threats via deception means you can minimize breakout time and containment time as well since the adversary has less time in your environment to move laterally and establish beachheads.

About the Author

Tony Cole, CTO, Attivo Networks. He is the Chief Technology Officer at Attivo Networks responsible for strategy and vision. He's a cybersecurity expert with more than 30 years' experience, a bachelor's degree in computer networking and is a CISSP. Prior to joining Attivo Networks, Mr. Cole served in a number of executive roles at FireEye, McAfee, and Symantec. He's retired from the U.S. Army and was an early advisor to Wall Street on the Cyber Security market. Mr. Cole serves on the NASA Advisory Council, the (ISC)² Board of Directors, and he's also a former president of ISSA-DC. In 2014, he received the Government Computer News Industry IT Executive of the Year award, and in 2015 he was inducted into the Wash 100 by Executive Mosaic as one of the most influential executives impacting Government. In 2018 he was awarded the Reboot Leadership Influencer Award in by SC Media. Mr. Cole is also a volunteer member of the WhiteHat USA Board, a charity benefiting Children's National Medical Center.

Tony can be reached online at (@nohackn, www.linkedin.com/in/wmtonycole) and at our company website https://attivonetworks.com/



Defending Forward

Human-Machine Teaming for Automated Predictive Prevention at Scale

By James Wallace Hess, Director of Development, Cythereal

Today's threat landscape demands automated analysis and predictive prevention to efficiently harden protection structures so that they can identify and disrupt attacks, proactively and at scale. The scope of the current problem is daunting. Threat intelligence companies process hundreds of thousands of malware samples every day. It is not feasible for threat researchers to manually analyze each sample, identify those relevant to an organization, and quickly extract indicators which proactively strengthen defenses. Faced with limited time and talent we must let go of relying on highly skilled experts to complete rudimentary tasks. Automating these tasks closes the gap with the Adversary, decreases time to detection, and accelerates time to prevention. It allows experts to concentrate on decisive prevention of the most dangerous threats. Automation offers the tools needed to decide in time to disrupt the next attack; to "Defend Forward". (1)

Automation cannot stand alone. It is an enabler which informs the expertise, humanity and creative talent of protection professionals. Automation provides the inputs necessary for them to apply their talents and effect rapid employment of proactive countermeasures. Through deliberate human/machine teaming, bias-to-action is realized by decreasing time to actionable decision options and achieving proactive response.

Many current methods focus on identifying Indicators of Compromise (IOCs) compiled from known breaches that have happened elsewhere. By definition, such measures are reactive because they are created from post-attack threat information. Not to diminish their importance; these are essential prevention methods for known malware. However, they fall short of efforts to get ahead of the Adversary as they do not customize protection or anticipate attacks. This is especially true when considering structures to prevent Targeted Attacks against an organization. The Tactics, Techniques and Procedures (TTPs) of the Adversary are designed to defeat generic IOCs.

We can infer from the threat model *(Threat) = (Capability * Intent)* that a reduction in the dimension of either capability or intent will degrade the aggregate threat level. For protection to succeed we must detect and respond faster than the adversary in order to disrupt the adversary's operational cycle. The earlier we disrupt the more the adversary must do to restore capability to the previous level.

Targeted Attacks are the most dangerous as they have inherent intent and persistent enrichment that improves their capability until successful. Here the Adversary proactively improves; learning

from failed attacks. We can exploit this TTP by using AI to learn from these failed attacks in time to generate reliable decision options.

Automation provides a marked advantage because, in a Targeted Attack every persistent attempt leaves behind the Adversary's exploit code. This is the weakness in the Adversary's operational cycle where capability can be disrupted and degraded. Further exploration of the Adversary's TTPs in a Targeted Attack confirms reuse of code as an economic necessity. Manufacture of new exploits is costly. The Adversary has learned that modifying existing code is the fastest and cheapest option. Capability is increased through variation and obfuscation of existing malware through repeated attacks until

penetration is achieved. Predictive technologies which can counter these techniques must be adopted if we want to proactively defend.

If the Adversary cannot be eliminated we must focus efforts on degrading the Adversary's capability. We must get ahead by predicting next-attack prevention options from the just-blocked attack where we are in contact. This keeps the engagement on the proactive side of the fight. Machine Learning allows us to put prediction on patrol, scouting for malware indicators, harvested from interrogation of just-failed attempts. From these indicators we gain the information about the next attack needed to Disrupt; resetting the Adversary's operational cycle. Capability denied yields a threat score of zero.

Among the thought leaders trying to provide a strategic edge by proactively combating malware is my company Cythereal. We got our start in the DARPA Cybergenome Project where we tracked malware genealogy. When an Independent Verification and Validation by MIT Lincoln Lab assessed that our system had the capability to predict future variants over generations of evolution and obfuscations, we realized it was our duty to develop the capability into a product. Our mission is to be the leader in predicting and preventing advanced malware attacks by leveraging code sharing and reuse to get ahead of the Adversary. We attack the Adversary's capability by defeating new variants through prediction. The increased time it takes the Adversary to achieve success affords defenders more time to anticipate, prepare, and maintain the proactive defense.

Cythereal's ability to predict variants is documented in a case study reported by McAfee Labs. (2) In this study, our MAGIC Early Warning System was fed a stream of malware blocked by McAfee End-Point Security (ENS). As concluded in the study, "MAGIC … found two Oceansalt variants from the wild which were not previously reported by the McAfee SOC or any other global threat intelligence."

Cythereal provides decision options for the threats most likely to succeed. Connect with us and get ahead of the adversary by pivoting your reactive defense to Defend Forward.

We encourage you to explore our enrichment by visiting our website and links below which highlight the use case from our McAfee integration and our collaboration with Deutsche Telecom. These show how we identify and defeat "previously unseen strains… before they can report to their C2." (3)

References:

(1) https://www.defense.gov/explore/story/Article/1891495/dod-more-assertive-proactive-in-cyber-domain/
(2) https://www.mcafee.com/blogs/other-blogs/mcafee-labs/did-you-check-your-quarantine/
(3) https://www.cythereal.com/wp-content/uploads/2020/01/DTAG_Insert.pdf

(4) https://www.cythereal.com/mission/
(5) https://www.mcafee.com/enterprise/en-us/partners/security-innovation-alliance/directory.html
(6) https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

About the Author

James has over 20 years of experience in technology ranging from Cyber Security, Image Recognition, and Data Science to Aviation, Intelligence, and Technology Management. He is the Development Director for Cythereal, a Louisiana Cyber Security Startup which uses Data Science to anticipate Cyber Attacks. He is also an Intelligence Officer and Aviator currently serving as Innovation Officer for the 75th Innovation Command's Austin Group. In addition to his Master of Information Technology, James holds an MBA, Master of Global Management, and Master of Business Analytics. He is has taught at Auburn University and is currently teaching in the Cyber Security Program at Tulane University. His research interests include Remote Sensing, Sentiment Analysis, and Image Recognition. He is a member of InfraGard, The Association of Old Crows, and Delta Mu Delta. In his free time James enjoys westerns, sailing, and history.

James can be reached online at james.hess@cythereal.com and at our company website www.cythereal.com .

Microsoft Brings Application Isolation to Office 365 with Application Guard

Users No Longer Have to Choose Between Security and Productivity

By David Weston, Director of OS Security, Microsoft

At Microsoft, we spend more than $1 billion annually on security and have more than 3,500 dedicated security professionals. Among them is a dedicated Offensive Security Research team, think of them as penetration testers specifically targeting our own products so we can design them more securely from the start. Every day, that team emulates and builds on known and evolving attacker techniques, trying to break into our own products. Findings are reinvested in our always up-to-date Windows 10 and Office 365 ProPlus product development, shared with the IT and security communities.

Among the most common and powerful attack vectors we have seen are those that exploit the daily tradeoff users make between productivity and security. Often, this is as simple as a document hiding an exploit or a malicious link. Basic phishing techniques or the simple pressures of a busy day can be enough for a user to open a file, dismiss security defenses like Protected View, and expose themselves and the rest of the network to attack. Many long-established security tools and practices consider this tradeoff inevitable.

We have machine learning and AI built into Office today that quarantines malware in email and file attachments, and there are policies we recommend as part of Microsoft Secure Score that will stop a lot of attacks, but nothing is perfect for all files, especially as attackers are constantly changing the techniques. Security always has to be evolving and working to proactively defend against exploits and get ahead of bad actors.

To do this, we've built more proactive protections into Office 365 and eliminated the need for users to have to choose between security and productivity. **Microsoft Defender Application Guard**, first introduced this hardware-level containerization with Edge and we continue to build on the concepts of isolation and minimizing trust by extending these capabilities to Office 365 applications. With Application Guard for Edge, if a user visited an untrusted website, Application Guard enabled Edge to deliver that site in a container, with a new instance of Windows and entirely separate copy of the kernel. Application Guard's enforcement completely blocked access to memory, local storage, other installed applications, corporate network endpoints, or any other resources of interest to the attacker. Now, these capabilities will be available to Office documents.

Microsoft Defender Application Guard for Office 365 enables users to stay safe, secure and productive when working with untrusted documents. It's built directly into the Windows platform so users get a native, seamless experience where they can continue to work as they normally would.

This hardware-backed security isolates untrusted Office documents without compromising the comfortable experience to which Office users are accustomed because it is built directly into the Windows 10 platform. With Application Guard, an untrusted document that is opened inside the Application Guard container has the same look and feel as an Office document opened on the desktop.

Now, users can open an untrusted Word, Excel, or PowerPoint file in a virtualized container, and view, print, edit, and save changes to untrusted Office documents – all while benefiting from that same hardware-level security. If the untrusted file is malicious, the attack is contained and the host machine remains untouched. A new container is created every time you log in, providing a clean start and peace of mind for both users and cyber security teams.

If users do need to "trust" a file to open it with more privileges, files are automatically checked against the Microsoft Defender Advanced Threat Protection (ATP) threat cloud before it is released. This integration with ATP provides admins with advanced visibility and response capabilities – providing alerts, logs, confirmation the attack was contained, and visibility into similar threats across the enterprise.

About the Author

David Weston is the Partner Director of OS security at Microsoft where he is responsible for the Security engineering of Windows, Windows Server, and the Azure OS as well as the Offensive Security Research Team (also known as the Windows RED TEAM). Before leading security engineering in Windows, David led the security research team for Microsoft Defender Advanced Threat Protection (ATP), the team responsible for detecting and responding to global adversaries. David has been with Microsoft since Windows 7, holding many different security roles in mitigation design, penetration testing, malware analysis, and threat intelligence. In addition to his engineering work, David is also an accomplished security researcher presenting his work at numerous security conferences including Blackhat and Defcon. Learn more about David https://news.microsoft.com/

Autonomous airtight security for your network at scale

Zero Networks holds the key to your network security, enabling you to quickly and effortlessly achieve a zero trust network model at scale. With the click of a button, you have tailormade user access policies for your entire network. Everything is automated - there are no agents to deploy, no policies to manually configure or update, just airtight network access security for everyone, everywhere.

ZERO.
Networks

www.zeronetworks.com

The Evolution of PAM: Why Just-in-Time Administration Has Changed the PAM Game Forever

By Mahesh Babu, Sr. Director and Head of Product Marketing at Remediant

When assessing an organization's cybersecurity posture, privileged accounts are the most critical to safeguard because of their proverbial "keys to the kingdom." Malicious digital insiders who are able to gain access to these privileged accounts are able to exploit them through lateral movement once inside the network. If attackers can get in through the interior of a network, the lateral movement can be crippling to a network's defenses. Attackers can gain access to personal and sensitive data, putting millions of customers at risk, along with your brand's reputation.

To solve this issue, privileged access management (PAM) vendors launched a variety of offerings to market about 20 years ago. Unfortunately, even with enterprises adopting PAM, we still hear of data breaches almost every day of the week. The value of PAM was never fully realized for five key reasons:

1. **Focused on authentication, not access:** Legacy PAM solutions focused exclusively on authentication as the method for protecting privileged access. Over time, innovation in these legacy PAM solutions has involved longer passwords or more frequent credential rotation – but never quite addressed the real needs of practitioners who use these solutions every day. **Outcome:** High residual risk, high friction
2. **Undiscovered, always changing privileges:** PAM solutions protect known privilege. They do not offer a way to discover and monitor privileged access across the enterprise. This results in an invisible sprawl of administrator privilege ready to be compromised and completely unknown to an organization. **Outcome:** Unknown attack surface
3. **Unnecessary standing access = Larger attack surface:** Administrators have 24x7x365 access to company networks, so all it takes is one hack, one single credential stolen, and then the attacker has the "keys to the kingdom." From there, an attacker can move laterally to steal IP and other sensitive data from HR, finance, R&D and other critical systems. **Outcome:** High residual risk

4. **High friction user experience for privileged users:** Accounts managed through legacy PAM have to check out a generic or shared ID and get approval every time there is a need for privileged access. **Outcome:** This approach slows down their ability to respond quickly, thereby increasing Mean Time To Respond
5. **Consistently incomplete deployments:** An agent-based approach that requires touching each endpoint in a network does not scale. This, coupled with high administrator friction results in incomplete PAM deployments. The problem is further exacerbated as workloads are dynamically provisioned and are ephemeral.

This is why, according to Forrester Research, up to 80 percent of breaches involve compromised credentials.

The Verizon Data Breach Investigations Report (DBIR) found that out of all attacks – 29% of total breaches involved the use of stolen credentials – second only to phishing. Current approaches to password security and PAM are obviously not enough. Simply put, PAM needs to evolve and the answer is Just-in-Time Administration (JITA).

Industry Validation

For the past two years, Gartner has ranked PAM as the number one security project and that's not surprising since most data breaches today are due to compromised, weak and reused passwords. Gartner also issued a September 2019 report, "Remove Standing Privileges Through a Just-In-Time PAM Approach," that states, "To properly mitigate the risk of standing privileged access, security and risk management (SRM) leaders responsible for IAM should closely follow the vision of the principle of least privilege and drastically reduce, with a goal toward eliminating, standing (i.e., "always-on") privileged access by using just-in-time (JIT) approaches. This will ensure that privileges are only granted when a valid reason for them exists, with zero standing privileges (ZSP) as the goal."

When user and machine accounts have standing or persistent privileged access, it creates the opportunity for threat actors to move laterally inside a network, even with a password vaulting solution in place. Zero Standing Privileges (ZSP) render privileged accounts useless to unauthorized users, even if they possess the credentials. ZSP leverages a Just-in-Time Administration (JITA) approach to reduce the attack surface and stop privileged account abuse.

PAM security firm Remediant pioneered the JITA approach years ago to effectively secure enterprises against administrator credential theft attacks that have caused some of the most devastating breaches to date. Remediant offers a patent-pending, JITA approach to solving credential theft attacks through the removal of standing privileges, which fundamentally reduces the attack surface for enterprises. As a result, Gartner also named Remediant a Cool Vendor in Identity and Access Management last year.

The Benefits of JITA Explained

JITA allows system administrators to grant users privileges to resources for a limited period of time, in order for them to log in and address an issue, and then rescind that permission. Making admin access more dynamic — granting it only when and where it's needed — prevents persistent access

that can open the door for data breaches. To add another layer of protection, this Just-in-Time approach can and should ideally be paired with two-factor authentication. This strategic approach gives the administrator the credentials they need, at the moment they need them, and configures permissions to expire after a specified time period to enable optimal security.

Incumbent JITA Approaches Do Not Solve the Problem

Recently announced just-in-time access approaches by legacy PAM vendors do not solve the problem if access is granted universally. “Just-in-time access to everything” does not mitigate the risk of compromised admin credentials.

Introducing Zero Standing Privilege

Remediant’s SecureONE PAM takes a precision approach to JITA and administers access to the right system at the right time. We do this by establishing enterprise-wide Zero Standing Privilege as follows:

1. **Establishing continuous inventory and compliance:** SecureONE constantly scans for privilege access across the ecosystem, acting as a single source of truth for reporting the distribution of privileged access **(150,000 endpoints in sub 2-3 hours)**.
2. **Locking down lateral movement and ransomware spread:** SecureONE removes standing privilege with a single action at a few milliseconds per endpoint.
3. **Reporting on the State of Privileged Access:** SecureONE continuously reports on how privileged access risk has evolved over time across the enterprise.
4. **Enforcing Just-in-time administration with MFA** without adding any friction to current admins or current processes.

With credential-based breaches at an all-time high, we need a shift in security strategy. Legacy PAM (both vault and JITA) leave us exposed to the risk at unacceptable levels.

It is time we rethink data breach control through the lens of privileged access. With Remediant’s Zero Standing Privilege approach to PAM, companies can gain the upper hand in cybersecurity defense once again by changing their perspective from not just who should have access to what, but when and for how long they should have access. For more information on Remediant, please visit: https://www.remediant.com/

About the Author

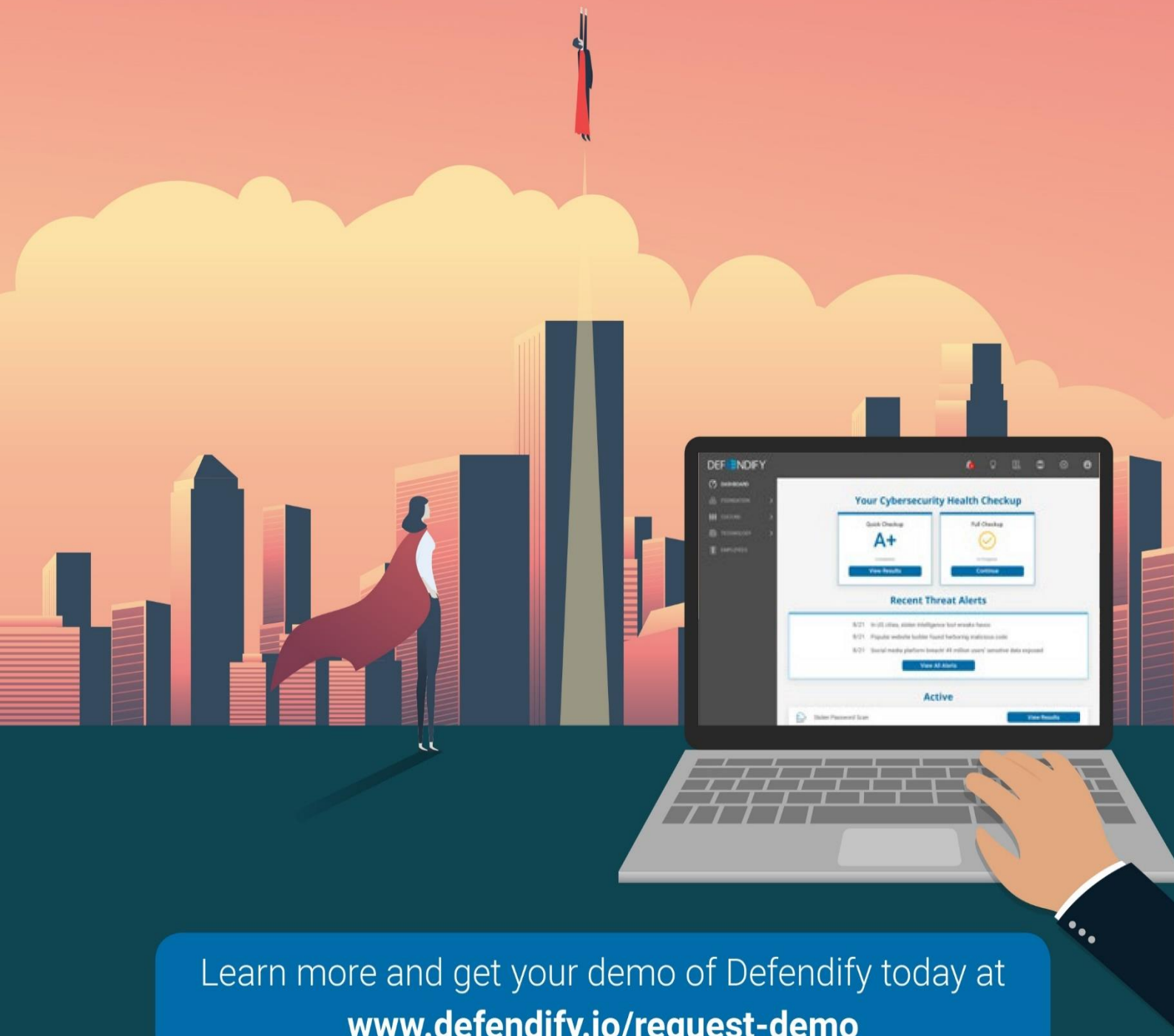
Mahesh Babu leads Product Marketing for Remediant. He takes every opportunity to tell everyone how Remediant has fundamentally changed Privileged Access Management (PAM). Prior to Remediant he spent time at Contrast Security as the GM for their RASP business growing it from launch to 50+ customers and most recently built out their Global Product Marketing team.

Mahesh has seen the industry evolve as a researcher, consultant, practitioner within a large bank. He began his career as a security researcher at the CERIAS center at Purdue University. He then went on to build and scale large IAM programs at HSBC (which included a painful PAM project). He also spent time at Symantec, Deloitte, Booz & Company. Mahesh has a BS in Computer Science and MS in Information Security from Purdue University and an MBA from Duke University.

DEFENDIFY

Cybersecurity. *Simplified.*

The All-In-One Cybersecurity Platform for Small Business.



Learn more and get your demo of Defendify today at
www.defendify.io/request-demo

Defendify • 175 Lancaster St., Suite 216, Portland, ME 04101 • www.defendify.io

GDPR stand aside -- meet CCPA!

The interactions between CCPA compliance and Security solutions.

By Oren T. Dvoskin, Global Marketing Director, Sasa Software

Introduction

The California Consumer Privacy Act, AB 375 (”CCPA”) was enacted in June 2018, and became effective on January 20th 2020. CCPA’s provisions potentially reach far beyond the European Union’s General Data Protection Regulation (“GDPR”). Accordingly, now is the time to review and assure compliance with CCPA, especially for those organizations who have relied on GDPR compliance to avoid regulatory penalties.

Although strong security infrastructure is vital for CCPA’s additional requirements, unless it’s carefully monitored, it can still be a source for data loss. In this article, we discuss how Content Disarm and Reconstruction (“CDR”) can help with both regulatory compliance and effective protection against data loss and additional adverse consequences.

Together, implementing measures to meet these regulatory standards, as well as taking all steps to assure the confidentiality, integrity, and accessibility of sensitive data, can make the difference between an industry leader and a competitor who’s always trying to catch up.

Meet CCPA

California has always been known as a progressive State for protecting consumer rights and individual privacy. While this has been beneficial in many ways for its residents, new laws and regulations have also opened an opportunity for private action litigators to challenge companies for non-compliance. Companies must ramp up to protect themselves, especially given the extensive fines that can be levied for violations. The act imposes up to a $7,500 fine per breached record, and the penalties can grow exponentially over time with accumulated incidents. Beyond data protection,

CCPA is intended to *provide transparency to how information is used* and ensure that data maintained is both securely held, and also easily accessible.

CCPA's Privacy Impact and Reach

The CCPA regulations require companies to provide broad transparency in how they collect, share, and use all personal and consumer data collected starting from January 2020; and business to business (B2B) data is covered beginning in 2021. Consumers will have the right to access personal data collected in the last 12 months, categorized between sold and transferred, to enable them to understand how groups of companies share information to build behavior, attitudinal and predictive profiles. Data requests to consumers must be provided in a timely manner and in a user-friendly exportable format. Companies will be forced to build infrastructures to meet these mandates. Companies will also be obligated to provide opt-out choices to restrict selling or sharing consumer data with third parties. These opt-out links must be prominently displayed on their websites. Under certain conditions, consumers can demand the deletion of personal data from company data stores.

While CCPA is being touted as California's GDPR – it isn't only limited to residents of California, since it covers almost all organizations and companies working out of California. With tech giants such as Facebook, LinkedIn, Google and Apple all California based, the impact of CCPA is potentially global. Companies that have already invested to support GDPR may have a head start. While there is some overlap between GDPR and CCPA, several policies, processes, and systems will still need updating to address differences between the two laws; primary among them is the requirement for transparent public access to all personal records stored by companies, including a full listing of all third parties the information has been shared with. Companies have a 30-day time window to remediate violations reported by regulators or private individuals.

Security impact

A sound IT security infrastructure is the basis of preventing data exfiltration and also the basis of minimizing the exposure to CCPA violations. Yet the security systems themselves must not be a source of data leakage, and shouldn't be vulnerable to a third party with whom privacy information is shared. With the dramatic adoption of cloud-based security services, this requirement is becoming increasingly challenging to enforce.

According to the Verizon Data Breach Investigation Report (DBIR), weaponized documents are a primary attack vector on organizations leading to hacking-related data losses. As an example, in mid-December 2019, the Israeli Cyber Command issued a warning following dozens of incidents where sensitive documents were found on multiple cloud-based malware analysis platforms. The files were invariably uploaded by the security solutions deployed by the organizations, as well as by security analysts wishing to query specific files. Rigorous scanning, especially of otherwise undetectable file-based attacks, is a necessity to overcome such vulnerabilities.

Enter Content Disarm and Reconstruction (CDR)

Content Disarm and Reconstruction (CDR), is an effective technology for the prevention of undetectable file-based attacks since it transforms all incoming content into a harmless copy that

can be used safely. As reviewed by Gartner in their recent Hype Cycle for Threat Facing technologies, “CDR protects against exploits and weaponized content that has not been seen before.” Israel’s Defense Forces, Intelligence Agencies and Critical Infrastructures were early adopters of CDR, establishing it as fundamental security best practice.

Sasa Software, owned by Kibbutz Sasa in Israel, has established itself as the leader of this technology, helping to extend it from governmental usage into commercial applications. Sasa Software’s GateScanner CDR combines highly optimized Multi-AV scanners, together with NextGen detection, to prevent known and advanced malicious attacks. These modalities are integrated with proprietary file reconstruction to prevent undetectable attacks, including Zero Day Exploits and Ransomware, while maximizing both security and usability of the resulting files. The technology protects extensive use cases including portable (USB) media, Email, Document uploads, Browser Downloads, Network Segmentation and more. The solution can be deployed as a service (SaaS) as well as to protect OT and ICS networks.

GateScanner was initially designed to protect air-gapped networks, so it was built without requiring internet access or 3rd party cloud connectivity. All operations are done in a highly secure physical or virtual appliance that is disconnected while processing files. With a design based on strict security and privacy measures, the solution also returns to the safe “Zero State” after every scan, never storing copies of the information that was processed. GateScanner can also assist with the prevention of information leakage since the process can be applied in “DLP” mode, scanning outgoing files and enforcing privacy policies.

Conclusion

Preparation for CCPA requires both dedicated transparency protocols, as well as careful selection of cybersecurity infrastructures. Scrutiny should be applied when determining the effectiveness of the security provided by solutions, and how they address the privacy issues required by CCPA. Documents and files are vital for the working of every organization, yet are a key concern as a security vulnerability, as well as a potential source for privacy losses. Sasa Software is a world leader in CDR and integrates both security and privacy procedures that are effective in protecting organizations against advanced attacks and achieving privacy compliance.

About the Author

Oren T. Dvoskin, is the Global Marketing Director of Sasa Software, with over 10 years of business development, sales and entrepreneurial experience. Prior to Sasa Software, Oren was the business development manager of BeatMed Inc., a leading online marketplace for healthcare. Prior to BeatMed, Oren held leadership positions in the medical devices and healthcare industry. His business experience was preceded by an extensive R&D career, including management positions in the Israeli Air Force. Mr. Dvoskin holds an MBA from the Technion, Israel Institute of Technology and an undergraduate degree in Computer Science from The Interdisciplinary Center, Herzliya.

He's an avid cyclist and social activist, having represented Israel in the Summer Deaflympics.

Oren can be reached at orend@sasa-software.com, **LinkedIn:** linkedin.com/in/ordvoskin

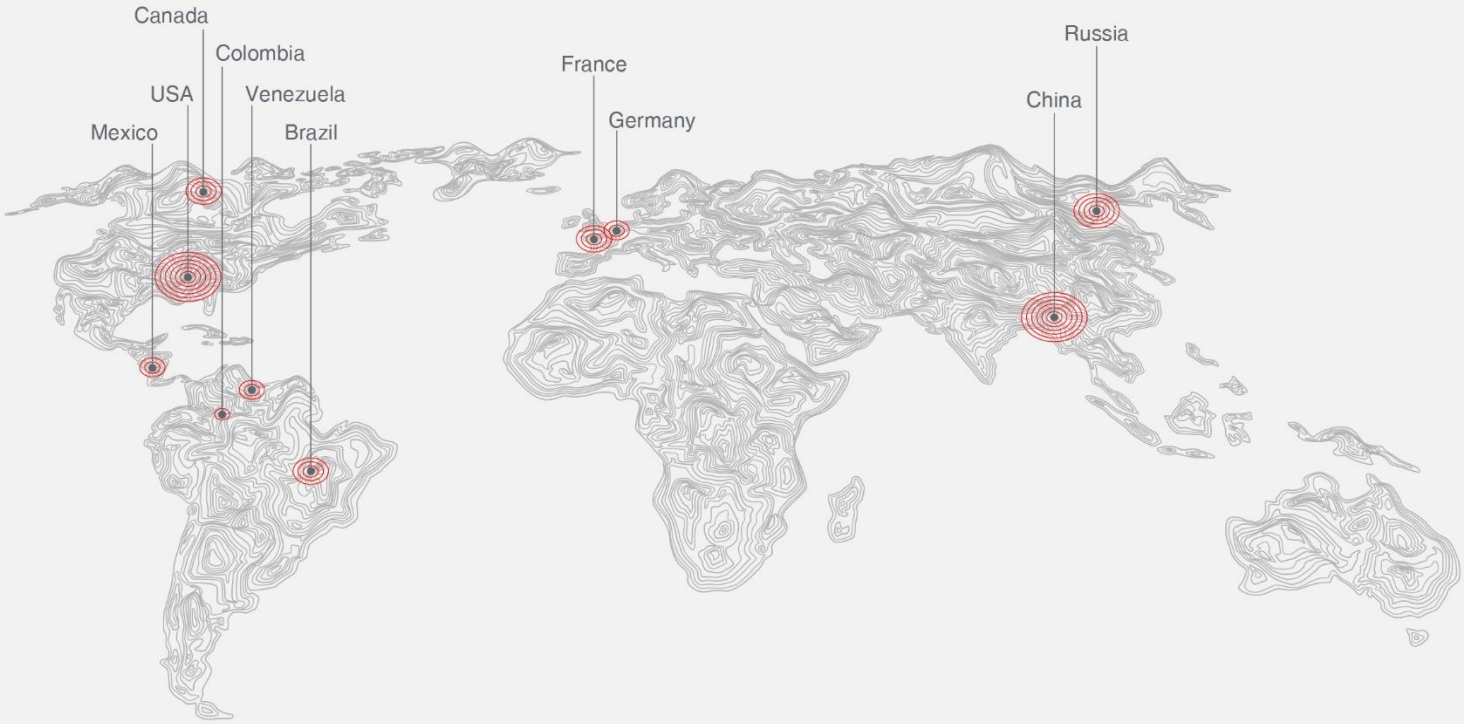
Or at the company's website: www.sasa-software.com

Oren T. Dvoskin | Global Marketing Director
Mobile: **+972.52.356-9591** | Tel/Fax: +972.4.867-9963
Kibbutz Sasa, m.p. Upper Galilee, Israel 13870
orend@sasa-software.com | **www.sasa-software.com**

2019 Cyber Attacks

NUCLEON®

Statistics of Cyber Attacks



1 USA
2 China
3 Russia
4 Brazil
5 France
6 Germany

Nucleon is monitoring and tracking cyber attacks around the world 24/7 and analysing them. During 2019 many sophisticated cyber attack compaigns have been seen.

Nucleon Created a complete framework that allows it to collect and analyze threat intelligence in reliable and quick way that have not been done before.

By inventing its own decoy systems (Polymorphic Sensors ,patented) Nucleon is able to collect reliable information regarding cyber attacks on the internet.

Nucleon developed a network containing proprietary data awareness algorithms using existing technologies such as graph databases and proprietary technologies such as Neural Networks.

contact@nucleon.sh **www.nucleon.sh**

5 Ways Hackers Can Bypass Your MFA

Think Your Sensitive Systems Are Secure? Think Again.

By Dana Tamir, VP Market Strategy for Silverfort

Let me start by saying - you should be using MFA (Multi Factor Authentication) on Everything! Passwords are no longer enough to validate the identity of your users and MFA has been proven as the best way to minimize the risk of identity-based attacks. You should use MFA to secure all access to your most sensitive and most critical enterprise systems – if you have the option, implement it.

However, not all MFA solutions were created equal.

Originally, MFA solutions were designed for VPNs and then extended to support specific systems. They were designed to be implemented one system at a time. In today's dynamic and complex networks, where we need to secure access by any user to any sensitive and critical asset - this approach is no longer practical. The implementation challenges leave too many sensitive systems unprotected. It only takes a single unprotected system to enable a breach. Once an adversary compromises a system and gains a foothold in the network, there are numerous techniques the adversary can use to elevate privileges and propagate throughout the network until a target system is reached.

But even if you have implemented MFA – your systems may remain exposed. Take for example most of the MFA solutions for MS Windows. These typically protect only local console logon and RDP access. They cannot add a secondary authentication prompt if you access with Command line tools like PowerShell "Enter-PsSession" or "Invoke-Command," or non-interactive logons (i.e. Log on as a Service, Log on as Batch, Scheduled Tasks, drive mappings, etc.).

And guess what: Hackers do not typically use local console logon and don't need to utilize RDP access. The administrative interfaces mentioned above are much easier to exploit. In fact, we have documented cases where these exact tools were used to breach organizations and access systems that were "protected" by MFA solutions.

Here are five ways hackers can bypass your MFA solution and gain access to your most sensitive, most valuable, and most critical systems:

1. **Remote PowerShell:** Windows PowerShell remoting lets you run any Windows PowerShell command on one or more remote computers. PowerShell Remoting lets you establish persistent connections, start interactive sessions, or access full PowerShell sessions on remote Windows systems. If PowerShell remoting is enabled on the target machine, you can use the Invoke-Command and Enter-PSsession cmdlets to execute an interactive session on the target machine. During the session, the commands that you type run on the remote computer, just as if you were typing directly on the remote computer.
2. **PSExec:** This is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install software on the target machine. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling that otherwise do not have the ability to show information about remote systems. It can be used, for example, to run credential stealing tools like 'Invoke Mimikatz' on the target machine.
3. **Remote Registry Editor:** As the name implies, this is a service that enables remote administrators (or hackers) to connect to a desktop or server system and view/modify the Windows registry. The registry is a database located within the Windows operating system responsible for storing all the configuration settings for software applications, user preferences and more. The remote registry editor service allows you to add new keys, delete existing keys, edit keys, search, and import or export keys. Since this service can pose a security risk, many security experts strongly suggest that you restrict access or even disable the feature if it is not required for remote management purposes.
4. **Remote Local Computer Management:** This is a collection of tools that allow administrators (and hackers) to connect to a remote PC and manage local resources such as user accounts, services and the device manager. Most if not all Windows Local Resources can be accessed and managed remotely using this tool set that comes built into the windows base install. This is very handy and a great time saver when doing remote support. It is also handy for adversaries that have credentials with Admin rights on the remote machine they wish to manage since no MFA will be prompted to request a 2nd authentication.
5. **Exploiting the Lock Screen Bypass Vulnerability (CVE-2019-9510**): Disclosed in 2019, this vulnerability in Microsoft Windows Remote Desktop Protocol (RDP) can be exploited by client-side attackers to bypass the lock screen on remote desktop (RD) sessions. The vulnerability resides in the way Microsoft Windows Remote Desktop feature requires clients to authenticate with Network Level Authentication (NLA). When a network anomaly occurs it could trigger a temporary RDP disconnect, but upon automatic reconnection the RDP session will be restored to an unlocked state. The RDP session will be restored without considering the status of the remote system before the disconnection. An attacker can interrupt the network connectivity of the RDP client system, this will cause the session with the remote system being unlocked without providing credentials. See this blog for more information.

Secure Access Across All Interfaces

In order to ensure secure access across all your system interfaces, you should look for an MFA solution that focuses on the authentication protocols (like Kerberos, NTLM, SAML and OpenID Connect) - rather than an MFA solution that focuses on a specific system's authentication process.

One solution that enables this is Silverfort's Authentication Platform. Unlike most authentication solutions that are implemented system-by-system, and require a software agent or some kind of integration with the protected system's authentication process, Silverfort applies a holistic protocol-based approach towards secure authentication. Silverfort monitors all the access requests of all users and service accounts, across all corporate networks and cloud environments, and across all the authentication protocols – in a unified platform. It analyzes these access requests to continuously assess risk and trust levels and enforces adaptive policies to ensure only validated trusted users are granted access.

Due to the holistic architecture of the solution, and the fact it doesn't require agents, proxies or code changes, Silverfort enables you to secure any system and any interface to that system. This includes systems that couldn't be protected until today, like legacy and homegrown systems, critical IT infrastructure, file shares, databases and more. It also secures all the interfaces to your systems, including privileged access and the use of administrative tools like Remote PowerShell, PSEcex and more.

This innovative architecture is not only easier to implement, because it eliminates the need to deploy system by system, an approach that is no longer practical in today's dynamic and complex environments, but it also enables better security that provides complete coverage to your systems.

To read more about this visit www.Silverfort.com

About the Author

Dana is the VP Market Strategy for Silverfort, provider of the first agentless, proxyless authentication platform that enable secure authentication and zero-trust policies across all systems interfaces whether on-premises or in the cloud. Dana is a veteran of the cybersecurity industry with over 15 years of real-world expertise and leadership roles in leading security companies. She was recently named one of the top 25 women leaders in Cybersecurity of 2019. Prior to Silverfort, Dana served as VP Marketing at Indegy (acquired by Tenable in 2019). Before that, she served as Director of Enterprise Security at Trusteer (acquired by IBM in 2012). She also held various roles at Imperva, Symantec, Bindview, and Amdocs. Dana holds an engineering degree from the Technion – Israel Institute of Technology, in addition to a number of industry and vendor certifications.

Delivering IT Talent for Analyzing and Safeguarding Data

Prosyntix

Prosyntix is a specialized Talent Delivery Firm with a niche focus in Cybersecurity, Infrastructure, Cloud, and Data. We take a unique approach to deliver the right talent by focusing in a specific area and following a proven Service Delivery Methodology

Assess > Design > Deploy > Enable

Talent Services

Technology Risk Management	Information Security	Cloud
Infrastructure	Analytics	DevOps

Benefits

Prosyntix takes a specialized yet agnostic approach to deliver technology solutions. With the ever-evolving landscape within Cybersecurity, Engineering, and Analytics, our firm has carved out a deep understanding of these pillars to better serve our clients.

Along with talent services, we also have a fantastic partner ecosystem that allows us to engage and deliver Subject Matter Experts every step of the way.

- Subject Matter Experts with Specific Focus
- Proven Service Delivery Model
- Proven Recruitment Methodology
- Partnership with Cybersecurity Education Firm

Diverse Supplier

HUBZone
Historically Underutilized Business Zone
CERTIFIED

DOBE CERTIFIED
Disability-Owned Business Enterprise
Disability:IN

Statistics

- 175 Zettabytes of data expected by 2025
- The US to account for half of breached data by 2023
- 230,000 malware samples are created every day
- Worldwide spending on cybersecurity is forecasted to reach $133.7 billion in 2022
- XaaS (everything as a service), UX/CX (User/Customer Experience), and digital privacy will take center stage in 2020

Office Location

307 W Tremont Avenue, Suite 200

Charlotte North Carolina 28203

Engagement Solutions

Professional Services	Contract
Contract to Hire	Direct Hire

Stopping Fraud and Threats with XTN

By Guido Ronchetti, CTO of XTN Cognitive Security

XTN develops Behavioral-based Fraud and Threat Protection solutions designed to defend digital businesses. Our security solutions are Cognitive, using proprietary AI algorithms. We also employ behavioral biometric analysis, both to guarantee complete user profiling, and to evaluate and block anomalies and threats in real-time.

Our award-winning Cognitive Security Platform®, specialized in behavioral in-app protection, fraud protection, and digital identity areas, provides our customers with the highest level of security and a fast return on investment.

The XTN team, young, eclectic, and highly qualified, is constantly developing our solutions to remain one step ahead of adversaries.

XTN is a global company with offices in Italy, the USA, and the UK

Cognitive Security

In 2014, we selected XTN Cognitive Security as the name for our company. Cognitive Security is at the heart of what we do, and represents the technological approach used in the development of our solution. Our intent was predictive of a phenomenon that spread years later. Our intention was to explain that we transformed human skills into artificial intelligence, creating our solutions. Cognitive Security is the application of artificial intelligence technologies, modeled on human thought processes, to detect security threats. Our experience in cybersecurity has been digitized to offer real-time, autonomous, efficient, scalable, and accurate evaluation flows. Since learning

algorithms make it possible for cognitive systems to constantly mine data and knowledge through advanced analytics, our focus is to refine methods and processes continuously, so the system–learns to anticipate threats and generates proactive responses. Our collective experience in cybersecurity is encoded into our products. This enables us to process and analyze huge volumes of data and identify threats impossible for a human to detect.

Behavioral Biometrics

In a world where compliance requirements, reputation protection, UX-based differentiation, and cost reduction are top priorities for the vast majority of businesses, Behavioral Biometrics solutions are gaining traction. Institutions and industry leaders mention them as an effective way to migrate users to modern authentication flows, minimizing friction. Various industries are facing the same need: strongly identifying users and preventing Fraud, affordably and without added complexity.

It is important to clarify that when we talk about Behavioral Biometrics, we don't mean physical biometrics involving innate human characteristics (for example, fingerprints, face, or iris). Behavioral Biometrics is the discipline related to uniquely identifying and measuring patterns in human activities. The potential is to provide a powerful way to prevent identity-related fraud and malware-based or bot attacks. Our behavioral biometrics provides an effective way to improve your security posture without disrupting your users' experience–and without hardware requirements.

Our technology provides smart solutions identifying and measuring patterns. Patterns are activities that could be related to a device and how we interact with it, to a geo-location, or to service-related habits (the usual amount in a payment transaction, the day of the week or hour of the day the user usually operates, the functionality often accessed, etc.).

Our Cognitive Security Platform®–features Behavioral Biometrics as a central piece for our user-focused analysis. It allow us to continuously evaluate the anomalies in interacting with the service, allowing the required countermeasures to be dynamic, saving the user from unnecessary friction.

We continuously develop smart solutions that are easy to use, impactful, and cost-effective.

Technology fields

Cybersecurity skills, AI, and behavioral analysis allow us to ensure the protection of our customers' digital services and their users through the award-winning Cognitive Security Platform ®, which features in-app protection, fraud protection, and digital identity components.

Behavioral In-app Protection

In-App protection is a security solution implemented within an application to make it more resistant to attacks. When you distribute a security-critical app to consumers or to enterprise users, you want to be sure that no one can attack it. You should deploy technology capable of protecting the app itself and reporting to you if something goes wrong.

Modern In-App Protection should provide three features:

- Multiple threats detection: ranging from malware presence up to misconfiguration of security conditions inside the endpoint. It should provide runtime detection, evaluation, and reporting.
- Behavioral Analysis: It should use to analyze user behavior and detect anomalies.
- Active App Protection: It should provide active and configurable countermeasures within the application that will prevent your app from working under certain conditions. The main functionalities to implement should be obfuscation and encryption in order to protect the app's assets from reverse engineering attempts (even if the app is not running).

Traditional In-App focuses only on the application as an asset extrapolated from the context. What differentiates us is having a comprehensive vision that considers both the user who accesses the service and the service that is used.

Modern threats are not black and white. Recognizing them requires intelligent processes. Reporting is required to trust the effectiveness of the countermeasure.

At XTN, we have designed a Behavioral In-App Protection solution, using AI in the process of threat detection, providing intelligent tools to protect your app-based services.

Digital Identity

Our solutions generate an effective profile of your customers' digital identity using dynamic digital indicators and guaranteeing high levels of security, and a fluid user experience. Digital identity validation relies on different layers through the XTN Cognitive Security Platform®: behavioral biometrics features, endpoint trust, and cryptographic quantities. These layers help us align the authentication mechanism based on endpoint trust or risk eliminating any friction and include continuous behavioral analysis to recognize anomalies.

Fraud protection

The Cognitive Security Platform is a comprehensive fraud protection ecosystem. Our approach is to correlate different layers of analysis to obtain a holistic view used to detect fraudulent events. The platform considers the posture of the endpoint used to access a critical service, the digital identity of the user, and the risk profiling related to the business content of events. Our technology relies on artificial intelligence for accuracy. Our technology combines different needs that are mandatory in the fraud analysis space: Behavioral perspective, awareness of and insight into risk causes, flexibility, and real-time response. We address the challenge of providing visibility about fraud attempts coming from consumer-facing or internal critical services. The financial

sector is one of our reference markets, where limiting payment-related fraud is imperative. Other markets also need this protection. We are working in the automotive industry to protect digital services in the context of Connected Cars.

XTN offers a comprehensive set of solutions, protecting you from fraud and security threats while keeping your digital service easy to manage and transparent to your end user.

Contact us to discover more about what we can do for your business.

About the Author

Guido Ronchetti is the CTO of XTN Cognitive Security. In its career, he has been involved in designing several security products. In XTN one of its primary aims has been to apply machine learning models to behavioural related security problems.

Learn more about Guido at https://xtn-lab.com/https://xtn-lab.com/

A Green Database

By Chris Jordan, CEO, Fluency Security

Datacenters are basically toxic computer equipment in a constantly cooled warehouse. Their footprint is growing across the globe in places like Loudoun County, Virginia, a place not known for its cold weather. Much of this growth is based on companies not knowing how to be efficient in the cloud. The scaling of inefficient code and processes means significant amounts of computer resources are needed. To address this environmental impact, cloud code needs to be more efficient and smarter in how it scales. This is the aim of a green database.

Green Database Benefits:

- Less Environmental Impact (less systems, physical waste and electricity)
- Less Cost
- Faster Searches

Fluency has already invested six years in developing LavaDB to be a green database. Fluency's objective is to advance technology and change the economics of the log analytics industry. Fluency does not simply seek to lower the cost of log management and data retention; instead it aims to lower the cost until it is practical to ingest and analyze everything. A green database is the cornerstone of this mission.

Why the Cloud Needs to be Green

When we think of saving the planet, we think of climate change, carbon release and pollution. We blame things like our cars, drinking bottles and plastic straws, for what needs to be changed. But when we look at the Internet industry and how data is doubling in volume every two years, the processing, storing and searching of this database has a significant impact on the environment. Today's inefficiency is often seen by companies in the high cost of a cloud project, as there is a direct relationship between cloud cost and the physical cloud presence.

Cloud systems scale painlessly. You do not have to wait for a machine to be delivered, installed and configured. With a click of a button or a call of a process, a new system or drive is requested and put into use. The ease of this process allows companies to quickly scale a process to hundreds of machines. IT departments can allocate new storage without facility impacts or delays. The image of the cloud being somewhere else makes the physical issues of infrastructure transparent to the decision maker.

Scaling is a two-edged sword. There is unlimited power, but it comes at a price. Bad code, or the use plain average code, scales. And a small inefficiency scales to a rather large one quickly. This shows up in the electricity bill. But it also physically shows up in the growth of datacenters.

If you fly out of Dulles Airport in Virginia, you will see a growing landscape of datacenters. Datacenters house massive amounts of servers. The most notable part of a datacenter is an equal amount of air conditioning units. These oversized units compose entire walls, hidden behind vents. There is nothing cost-effective about placing datacenters in a Southern state.

Datacenters are called that, for their primary purpose is the storing of data, which doubles every two years. With the storing of data, the processes that use datacenters also move into the cloud. In order to reduce the environmental impact of datacenters, we need to reduce the cost of storing and analyzing data. The cost is environmental, but in reducing environmental impacts (number of processes and amount of storage), we also reduce the overall cost. Green databases are good for business.

What is Green?

What defines a green database? A green database needs to do two things. First, the compression of raw data to the stored data needs to be below 20%. This is consistent with the general rule of 1:8 compression. The difference between these two numbers is the database needs to provide high-availability/high-durability. Second, the speed of the database needs to be within the N Log N search. Besides storing data, the processing power to search and maintain the database impacts both why people use it and the electricity it needs.

Fluency's green database, LavaDB, aims at using one-eighth (12%) of the electricity and physical infrastructure derived from the raw data it receives. That is four times better than any other commercial or open source database being used today. This relates to a reduction of the overall datacenter environmental impact by 75%.

Fluency aims to make audit storage cost effective to the point that a company can save all their logs at a lower price than the equipment generating those logs. If you have ever paid a bill to a cloud SIEM vendor, you know this cost.

Learn more about us at https://www.fluencysecurity.com/

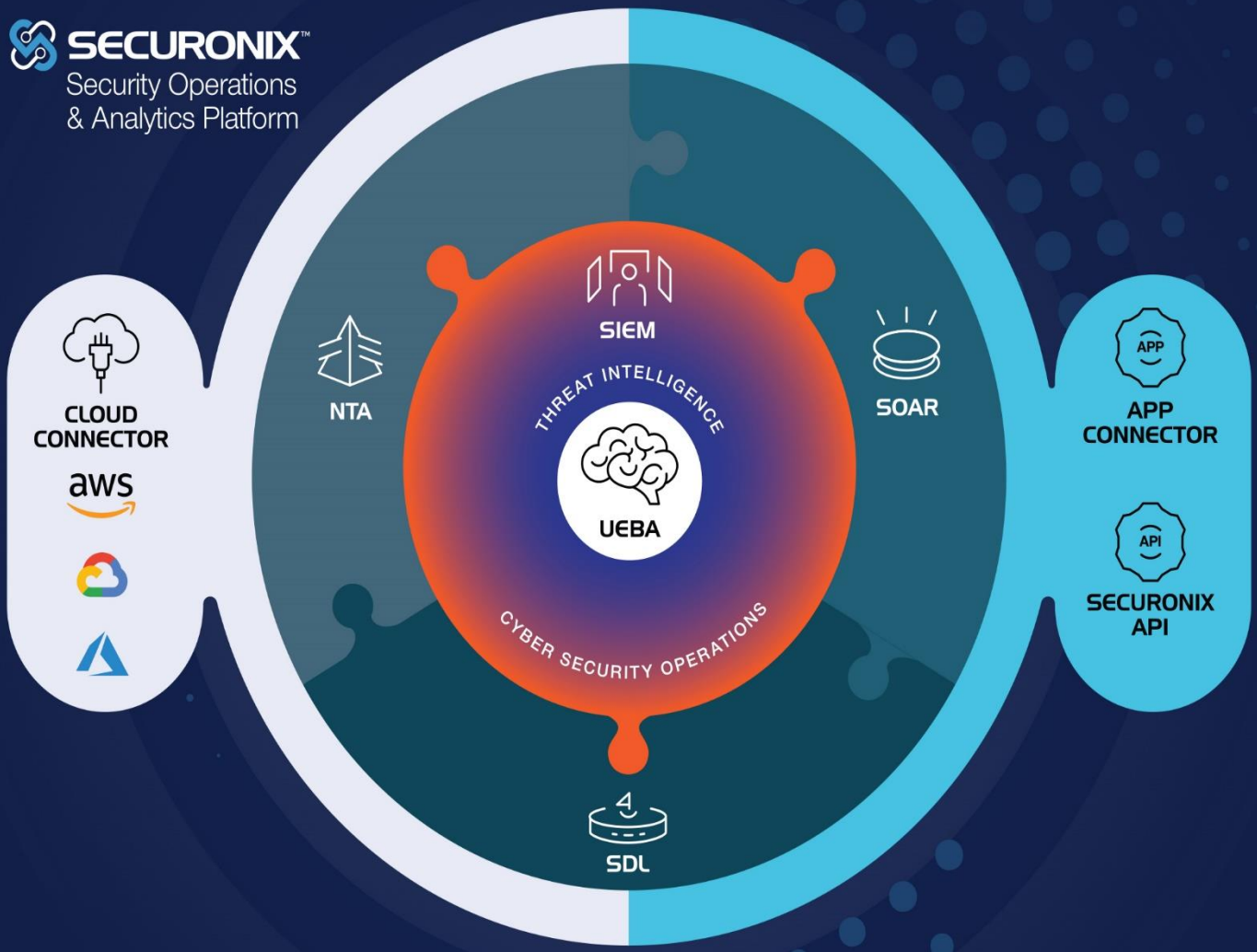
About the Author

Chris Jordan founded Endeavor Security, a cutting-edge, threat detection and analysis company focused on helping enterprises and governments protect their most sensitive networks. Acquired by McAfee in 2009, he then continued with a role as Vice President of Threat Intelligence. Well known for establishing some of the largest Government security operations centers, Chris changed his career, starting a security service company in 2003 and a research & development company in 2004. Both companies have since been acquired, and with retiring from McAfee in 2012 founded Fluency® with longtime friend and coworker Kun Luo.

Combat Threats in the **Multi-Cloud World**

Analytics-Driven Cloud SIEM

SECURONIX™
Security Operations
& Analytics Platform



The Securonix platform delivers analytic driven SIEM, SOAR and NTA, with UEBA at its core, as a pure cloud solution without compromise.

Securonix natively integrates with over 3000 3rd party vendors and technology solutions to simplify security operations, events, escalations and remediations

Find us at BOOTH #527

SECURONIX™

www.securonix.com

The Power of Purple

A Proactive Cybersecurity Paradigm

By Daniel DeCloss, CEO, PlexTrac, Inc.

Cybersecurity is hard, and attackers are relentless. The job of protecting an organization from cyber threats can feel overwhelming and stressful. The industry is short on talent and inundated with tools, vendors, and snake oil that further complicates the approach to building an effective security program. Despite these challenges, the expectations placed on the security team is to deliver a mature product that protects the organization's most critical assets. So, what can a team do to ensure they provide the value the organization expects with the limited resources of time, budget, and talent? This article cannot possibly claim to provide the complete answer to that question; however, we will discuss the paradigm shift needed with the most important piece of your security program – assessments.

We use the term assessment very purposefully. A security assessment is truly any activity conducted to determine the efficacy of a security control. Examples of assessments include penetration tests, vulnerability scans, risk assessments, compliance assessments, security questionnaires, etc. All of these activities have the purpose of identifying gaps in security controls and yet they are often disjointed activities and spread across multiple departments. Thus, the current assessment paradigm involves multiple assessments by multiple teams (internal or external) where security issues and gaps get identified and then handed over to engineers or analysts responsible for investigating and ultimately remediating the risk. This is a perfectly logical approach, but too often it is highly ineffective. The time it takes to conduct an assessment, deliver the findings, remediate the issues and then reassess the issues can take months if not years. Additionally, this is a reactive approach to

cybersecurity. In a world where threats and exploits change by the minute, we propose a better solution. That solution is proactive engagements through effective purple teaming.

To break down the new assessment paradigm, it's critical to break all functions and roles within your organization as either red or blue, where the composite of your entire team is purple (red and blue mixed, for the artistically challenged like myself). The red team is any team, person, or function that is proactively seeking gaps in the security posture. The blue team is conversely the function responsible for fixing those gaps and attempting to prevent new techniques. The old paradigm leaves little room for the blue team to be proactive on the prevention of new techniques, and it leave the red team in a position where they often report the same issue time and time again with little challenge to thwart new defensive measures.

Purple teaming, the new paradigm, reduces the mean time to remediation of security issues through centralized communication, effective collaboration, information sharing, and joint research. Let's dive into a thought exercise that highlights how this may actually occur within an enterprise security team. First, everyone must understand their function and role. The function is either red or blue, but the role is strictly purple, the common mission to prevent loss via a cyber-attack.

Second, there are no timelines with effective purple-teaming. Yes, there may be deadlines for compliance reporting or quarterly board reports, but attackers don't have cycles or timelines, and thus neither should the purple team. Proactive assessment is perpetual.

Third, red team activities must be targeted, specific, and focused. Yes, there are times when a full scope penetration test is going to occur, but that must always occur via an external team contracted to do so. The internal red team should always conduct exercises is small phases. For example, the red team may decide to evaluate the organization's capabilities for detecting or preventing certain attack techniques drawn from MITRE, such as a privilege escalation techniques related to DLL Search Order Hijacking (https://attack.mitre.org/techniques/T1038/). The ideal steps should be as follows:

1. Establish the test cases needed for evaluation
2. Communicate with the blue team the anticipated test cases and anticipated timeframe of the test
3. Execute the test and observe results
4. Communicate with the blue team on any findings and recommendations
5. Store these results in a central repository where both teams access, collaborate, and track the ongoing progress in real time.

These steps should happen in the matter of a week at most, then the blue team can quickly evaluate the results, prioritize remediation steps, and quickly execute the fix for expedited risk reduction.

Another example might be a red team activity of evaluating a security control related to PCI compliance. Let's say the red team wants to ensure the Cardholder Data Environment (CDE) contains proper access logs related to all administrators who access the system. The red team should execute steps 1-5 in a quick and iterative fashion, identifying the steps for evaluation and what evidence is needed. Then storing those results in the same central repository or platform for collaboration and tracking.

Fourth, blue team activities must be focused and disciplined to concentrate 70-80% of their efforts on proactive remediation. Today's current paradigm is to respond to alerts and events that come out of the SIEM or other alerting mechanism. The team then investigates, plugs the hole if it exists, and writes an analysis report. This is a very reactive paradigm and can turn into a never-ending cycle of reactive remediation. Instead, the optimal approach is to split resources within your blue team to be proactive and reactive where the proactive members represent a majority. These team members should be working closely with the red team to identify key gaps in the current security posture, and then researching additional mechanisms for remediation and any potential future threats that may result. The reactive blue team members should be working on responding to alerts and remediating the assessment findings.

For example, if the red team is testing privilege escalation techniques, the proactive blue team should identify what controls the organization has in place today and also research all possible techniques that might get used by the red team. They can then proactively implement the fixes independent of the red team's testing. Whereas the reactive blue team members should be monitoring logs and events in an attempt to identify the red team activities. This approach ensures that the organization is focusing on all aspects of the attack lifecycle from prevention to detection and response.

Finally, the most important piece to highlight in this paradigm shift is that assessments must move from single points in time to quick iterations and small but effective evaluations throughout the year. This ensures that at any point throughout the year, the purple team can take a snapshot of their current security posture to communicate to stakeholders. No more need to provide a document from six, nine, twelve, or even eighteen months ago, but rather a real-time look at progress being made today. The only efficient way to implement such a shift requires constant collaboration and tracking of the assessments on a daily basis.

In conclusion, the shift to a proactive cybersecurity program can be accomplished through the building of an effective purple team. This can start with simple mindset shifts about the functions of each member of the team, regardless of skillset. This paradigm shift is necessary and vital to truly shifting the needle in your cybersecurity maturity.

About the Author

Dan DeCloss is the Founder and CEO of PlexTrac and has over 15 years of experience in Cybersecurity. Dan started his career in the Department of Defense and then moved on to consulting where he worked for various companies including serving as a Principal Consultant for Veracode on the penetration testing team. Dan's background is in application security and penetration testing, involving hacking networks, websites, and mobile applications for clients. He has also served as a Principal Security Engineer for the Mayo Clinic and a Sr. Security Advisor for Anthem. Prior to PlexTrac, Dan was the Director of Cybersecurity for Scentsy where he and his team built the security program out of its infancy into a best-in-class program.

Dan has a master's degree in Computer Science from the Naval Postgraduate School with an emphasis in Information Security. Additionally, Dan holds the OSCP and CISSP certifications. Dan has a passion for helping everyone understand cybersecurity at a practical level, ensuring that there is a good understanding of how to reduce their overall risk.

Dan can be reached on LinkedIn at https://www.linkedin.com/in/ddecloss/ or on twitter @wh33lhouse and at our company website https://plextrac.com/

Is Data Loss Prevention (DLP) Really Dead?

By Uzi Yair, Co-founder GTB Technologies, Inc.

I recently came across several digital security vendor sites who describe themselves as a "DLP alternative."

Perusing through their pages, I came across comments such as "DLP is hard to deploy", "DLP is hard to maintain" and the classic: "DLP is heavy on the Endpoint". It's clear that these security vendors are trying to influence analysts by inserting these negative sentiments into the industry's discourse on DLP. Of course, terms such as "hard" or "heavy" are subjective at best and can't be taken as a concrete, professional assessment.

But my real issue with remarks like these is their shallow understanding of Data Loss Prevention.

Vendors and analysts tend to do a mediocre job explaining what DLP actually is.

Most people treat DLP as a single, specific product. In reality, DLP is a *set of tools* designed to protect data in various states. Here's my definition of what DLP is: A DLP system performs real-time Data Classification on Data in Motion and of Data at Rest and enforces predefined security policies on such streams or data.

This definition also requires us to flesh out our terms. "Data in Motion" means data on its way from a network to another destination, such as the internet, an external storage device (USB) or even to

printers or to fax machines. "Data at Rest" is data that resides in databases or any unstructured file anywhere on the network. "Data Classification" is the implementation of a *DLP policy* using specific markers--say, credit card or Social Security numbers for instance. These policies allow a given transmission of data to be placed in a specific category such as PCI or HIPAA.

From the definition above one can see that DLP is not a single tool, but rather a *set* of content-aware tools that include a wide range of applications including Network DLP, Endpoint Device Controls, Application Controls, and Data Discovery.

So Which Part is Dead?

Now that GDPR is in full effect it is hard to understand how Data Discovery is dead or even "seriously ill" as some observers have put it. One of the basic GDPR requirements is to inventory and classify data containing Personal Identifiable Information, or PII. Such data can reside in a wide range of storage areas including file-shares, cloud storage, or other in-house databases. Once the data are discovered, they need to be protected from dissemination to unauthorized entities. Far from being a thing of the past, DLP tools will play a vital role in achieving compliance with the most important set of data regulations ever to hit the world of information technology.

Today's DLP tools are designed mainly to protect PII.

This is a requirement of most data protection regulations in existence, such as PCI, HIPAA, CA1386, California Consumer Privacy Act of 2018 (CCPA), GLBA, GDPR, NY DFS Cybersecurity, PDPA, and SOX. But protection isn't as simple as guarding personal details stored on the network. Effective DLP requires a system capable of comprehensive Data Discovery. Achieving Data Discovery means understanding where all enterprise data is located, and to mitigate the risk of loss by various remedial actions such as:

- Changing Folder Security Permissions
- Moving/Coping the data to another secure folder
- Encryption
- Redacting images with sensitive data
- Enforcing Digital Rights Management
- Classification

In addition to these passive defense steps, DLP must also have ways of identifying threats and protecting against attacks on a network. Proprietary algorithms such as GTB's artificial intelligent programs can identify even partial data matches, managers remain alert to any attempts at data exfiltration from a malicious insider or malware. Though inaccurate in detecting data exfiltration, **User / Entity Behavior Analytics (UEBA)** together with intelligent DLP may be able to identify the presence of malicious programs on a system. In this way, systems, such as GTB's DLP that Works^{tm,} address the insider threat as well, ensuring that neither a company's personnel nor its digital applications become the means for compromising data loss.

The million-dollar question

But here's the million-dollar question: if DLP is so essential, why is it getting such a bad rap?

Let's try to understand where this negative perception came from.

Here are some of the end-user complaints as described by a Deloitte Survey entitled "DLP Pitfalls":

- "High volumes of false positives lead to DLP operations team frustration & inability to focus on true risks"
- "Legitimate business processes are blocked"
- "Frustration with the speed at which the DLP solution becomes functional"
- "Unmanageable incident queues"

These complaints stem from the fact that most DLP vendors have mediocre detection capabilities. This is because almost all systems use predefined data patterns, called templates, to locate and classify data on a system. While templates are easy to define and use, they produce waves of false positives that make the system useless from a practical perspective. Customers are left feeling they've bought an expensive toy rather than a system meant to secure their data. No wonder customers are frustrated by DLP capabilities or its value.

The dreaded False and Negative Positive

So, is it possible to solve the dreaded false positives dilemma produced by DLP systems?

Fortunately, the answer is yes.

Using content fingerprinting of PII and defining multi-field detection policies, such as combining last name and account number markers within a certain proximity, hones in on specific data and whittles away at irrelevant files. Using this multi-tiered scheme, the system detects the actual data of the company rather than just a data *pattern* that may or may not be relevant and has been shown to reduce false positives to almost zero.

While some DLP vendors support content "fingerprinting", they do not promote this technique for a good reason. The number of fingerprints produced can become so large that the system can crash, or at the very least slow down the network.

But this is not true for all DLP systems. GTB's proprietary fingerprinting technology allows customers to fingerprint up to 10 billion fields without network degradation.

And as for the concern, DLP systems are "unmanageable" and hard to use?

I disagree with the premise.

Even the more sophisticated functions of a DLP system such as running a select statement from one PII table while defining a multi-column policy in another field, are actually quite simple.

In summary

DLP is not just a singular tool and not all DLP systems are the same.

Contrary to the naysayers, the growth projections for the industry clearly show that DLP is not “seriously ill” and is definitely not dead.

Learn more about us at https://gttb.com/

About the Author

Uzi Yair,Co-founder GTB Technologies, Inc.

Uzi Yair, the co-founder of GTB Technologies leads the product development of GTB's game changing Data Protection platforms and solutions. For the past 13 years, Uzi has been advising and providing insightful guidance on all aspects of data protection, compliance and business strategies for some of the world's largest financial institutions, enterprises & government agencies. He is well knowledgeable and experienced in regulations and compliance standards including CCPA, GDPR, GLBA, HIPAA, HITRUST CsF, ISO 27001 and 2, NIST, NY DFS, PCI-DSS, SOX, and the like.

Database Cyber Security Guard

Prevents data theft by Hackers, Rogue Insiders, Phishing Email Attacks, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks when the security perimeter has been penetrated.

Average data breach in US costs $7.3 million dollars. Would have immediately shutdown the Equifax and Marriott hackers.

- Product Features -

- **Detects Oracle, SQL Server, DB2, Informix and Sybase data theft within seconds and immediately shuts hackers down.**
- **Dashboard view of hacker activity over any time frame.**
- **View all suspicious hacker SQL activity and data theft.**
- **Runs from a network tap or proxy server for non-intrusive detection of Data Breaches. Has no impact on databases.**

Advanced SQL Behavioral Analysis of the SQL activity learns what the normal SQL/query patterns are and stops the theft of data.

www.sqlpower.com/cyber-attacks

Securing the Next Generation Data Center

Dr. Ratinder Paul Singh Ahuja, Chairman of the Board & Chief R&D Officer ShieldX Networks

Securing Cloud-Generation Data Centers

As many firms transition their data centers into the cloud and/or heavily virtualized environments, the old practice of securing the perimeter from North-South data flows simply doesn't work. According to Gartner, by "2025, 80% of enterprises will have shut down their traditional data center, versus 10% today." Security, infrastructure and operations professionals need a new approach to network security for this overwhelming increase of East-West traffic where discovery, visibility, compliance and enforcement become impossible.

Available approaches such as agents and virtual firewalls, fail on several critical fronts. Only ShieldX can deliver a new network security platform providing automated policy generation, visibility and controls for Layers 3-7, microsegmentation with the click of a mouse and scalability across the multi-cloud.

Forward-thinking enterprises require a new technology to help IT and security deliver secure, agile services leveraging the promise of cloud economics. Cloud migration is happening fast—yet CISOs still need to maintain vigilance and control. And they must do it facing a significant skills gap both in cloud and network security. With ShieldX, enterprises leverage a cloud-native and microservices architecture to discover, automate and secure any workload, making digital transformation with Zero Trust one of the easiest things to implement in the cloud.

With ShieldX, infrastructure teams:

- Won't add environmental complexity
- Set and forget with a quick time to deploy and virtually no long term maintenance
- Don't require incremental resourcing

ShieldX Brings Cloud Generation Security to Multi-Cloud Data Centers

The ShieldX Elastic Security Platform was built to secure modern, multi-cloud data centers. It dynamically scales to deliver comprehensive and consistent security policies and controls to protect data centers, cloud infrastructure, applications and data, no matter where they are or where they go—to make the cloud more secure than on-premise deployments. ShieldX is the only cloud-native security platform that continuously discovers workloads, identifies risk, and enforces security policies for Amazon Web Services (AWS), Azure, and VMware in your multi-cloud environments.

Agentless Approach to Data Center Security. According to Forrester, the average cloud workload contains 20 agents, creating a management headache. Agent-based approaches are extremely difficult to operationalize, costing time and money for each instance. To make matters worse, agent-based solutions for microsegmentation don't actually perform security—they merely manage IP tables in hosts. And they cannot provide visibility unless deployed *a priori*.

ShieldX, on the other hand, provides a frictionless means to discover, automate, and microsegment all the way to Layer 7, providing visibility, security policy generation and controls within minutes of deployment. ShieldX sits at the network layer to discover all workloads and applications without needing to install a burdensome agent. ShieldX provides visibility without an agent. Enterprises can now execute microsegmentation and other cloud security initiatives quickly and efficiently, without needing to know where to deploy thousands if not hundreds of thousands of agents.

Visibility into Cloud Workloads, Threats and Vulnerabilities. With ShieldX, CISOs and CIOs can manage network security consistently across each cloud platform, creating one single console view. ShieldX continuously discovers all workloads in your multi-cloud environment, shining the light of visibility on your data center with a multi-tier, application-centric view across networks, virtual switches, distributed virtual switches, virtual private clouds, vNets, subnets, workloads, tags and much more. Then, ShieldX generates a mathematically precise set of policies and associated threat controls to provide visibility, threat prevention, microsegmentation, and security enforcement to eliminate the risk of flat networks. Using deep packet inspection, ShieldX investigates and classifies cloud traffic to understand attack surfaces. Finally, by integrating with vulnerability scanners, ShieldX assesses vulnerabilities and classifies data in rest as well as data in motion.

Intent-Based Automation. The ShieldX Adaptive Intention Engine quickly and effectively models relationships and entities to produce a visual application connectivity graph, allowing administrators a clear picture of their traffic dynamics over time to pinpoint potential issues. Our Elastic Security Platform then suggests a security policy based on the application connectivity model, which administrators can change and tune. For initial setup, the automated policy recommendation dramatically decreases the time to value for our Elastic Security Platform, allowing organizations to implement policies and protect resources in hours, not weeks. After implementation, ShieldX continuously and instantly updates policies and controls based on security intention.

A Full-Stack of Security Controls. ShieldX provides comprehensive security controls that go beyond basic network ACLs. Because ShieldX uses a holistic set of mitigations to keep the workload secure, a true defense-in-depth model for each microsegment is deployed, and multiple mitigation layers defend the attack surface intuitively, in unison, and with a layered approach. Controls include microsegmentation, URL filtering, malware detection and IPS/IDS.

Deploys a Zero-Trust Networking Architecture. ShieldX plays a key role in facilitating zero-trust networking. Microsegmentation combined with Layer 7 inspection and adaptive controls ensures only trusted users and applications can access specific systems and data, while extending the concept of zero-trust across all OSI layers. ShieldX delivers:

- Application-level visibility
- Automated network security policy
- Automated threat prevention security policies
- Automated control deployment

Elastic Scaling with Cloud-Native Microservices-Based Architectures. Unlike other options on the market, ShieldX uses cloud-native, containerized microservices to automatically scale elastically to any sized environment without suffering from performance degradation or reduced security. For example, when using a legacy virtual firewall, more TLS implementations could require the purchase and deployment of more full firewall licenses just for the expansion of that one feature. ShieldX, on the other hand, simply scales up the TLS microservice to whatever level is needed. This groundbreaking innovation provides an unparalleled ability to deploy security controls where and when they are needed, at any scale, without compromise.

Benefits

Slam the brakes on costs. ShieldX provides a single point of management for multi-cloud data centers to eliminate manual processes, control sprawl, and minimize ongoing maintenance requirements. Also, with ShieldX's automated policy generation and orchestration, enterprises easily avoid costly misconfigurations.

Stop wasting time. Manual policy generation is as mundane as it is time consuming. With ShieldX, security teams leverage automatic security policy generation to eliminate this tedious task and put that regained time to better use.

No more risky business. Maintain vigilance over cloud operations and workflows, reducing risk through a stronger security posture and more effective controls. With ShieldX, enterprises won't worry as much about imprecise policies or controls, or undetected changes stemming from separation of DevOps and security. Using continuous discovery and visibility into workloads, applications and data, enterprises mitigate the risks associated with flat networks and vulnerable systems across the East-West axis. This allows security teams to automatically protect multi-cloud data centers from ransomware and misconfigurations that result in data loss.

Elasticity That Scales with Your Business. Scale elastically to your business needs—seen and unforeseen— with comprehensive and consistent controls that protect your applications and data, no matter where they are, where they go, or how busy you get. With ShieldX's containerized microservices architecture, you can enjoy a cloud-native security solution that works the way cloud tools are supposed to.

Learn more about us at https://www.shieldx.com

About the Author

Dr. Ratinder Paul Singh Ahuja,Founder And Chief Research And Development Officer

Ratinder leads ShieldX and its mission as its central pivot point, drawing from a career as a successful serial entrepreneur and corporate leader, bringing with him his unique blend of business acumen, industry network and deep technical knowledge.

His previous three founded startups, Internet Junction, Webstacks and Reconnex were acquired by Cisco Systems, Extreme Networks and McAfee, respectively, where he subsequently served as Chief Technology Officer and Vice President of the Mobile and Network Security Business Units. His knowledge of innovation and emerging trends in networking, network security and data loss prevention are derived from years of industry experience. Dr. Ahuja holds a BS in Electronics & Electrical Engineering from Thapar University, in India and a Masters and Ph.D. in Computer Engineering from Iowa State University. Dr. Ahuja has been granted 37 patents for security-based technologies, and has presented in many public forums including the Content Protection Summit, IC3, IEEE Computer Society, McAfee FOCUS and the Cloud Expo.

Beyond his passion for technology and building new and exciting companies, Ratinder is a car enthusiast and a TaeKwonDo Master, with a 6th Degree Black Belt, practicing QiGong and weight training.

CASB+ Is Essential Infrastructure for The Cloud Mobile Digital Transformation

By Salah, VP of Marketing at CipherCloud

The ongoing cloud mobile digital transformation has brought cloud access security brokers (CASB+) front and center as an important part of enterprise cloud mobile security architectures. This article will take a closer look at the cloud mobile digital transformation, the new drivers for an improved cybersecurity architecture, and the benefits that CASB+ brings that make it both compelling and essential.

We've all seen the weekly barrage of news about the growing number of security breaches and the almost total failure of our legacy cybersecurity architectures. The transition to a cloud mobile world has happened faster than any of us truly anticipated and is part of the reason that many breaches have happened.

Today it is the new normal that your enterprise might have several cloud deployments, perhaps a mixture of private and public clouds hosting internally developed applications such as accounting, finance, or special manufacturing operations software, and public clouds providing software as a service (SaaS) applications such as Slack, Box, Office 365, Salesforce and others. Of course, this cloud mobile world requires that you administer each of these cloud environments separately. Each of them has different security capabilities. Of course, integration between these clouds and existing on-premise systems is the complexity icing on the cake. So many security stacks and very little in the way of consistency.

The explosion in IoT has been continuing with no end in sight. Internet of things (IoT) devices and integrated processors have brought many quasi-endpoints that can no longer be adequately protected. Standard software for endpoint detection and response (EDR) cannot protect many of these devices. There are many types of IoT devices. For example, the security systems that control door access, as well as the enterprise security cameras, are pervasive and yet even as part of your physical security infrastructure unwittingly provide many insecure points for potential cyber attackers to compromise.

In the healthcare industry, medical devices are similarly closed to 3rd party software. The FDA certification does not allow anyone to add any software to these devices so once again hospitals and healthcare institutions don't have any visibility to the threats that may lurk inside. And even in banking, large networks of automated teller machines (ATMs) remain targets of high value for motivated attackers. Many use IoT interfaces and all depend on special embedded processors to support ATM functionality. Point of sale retail networks suffer from the same IoT vulnerabilities. These IoT endpoints and the accompanying array of integrated devices overwhelm most security architectures. Just putting them "behind the firewall" is no longer enough to guarantee adequate protection. All of these allow attackers to quietly penetrate your networks, and then to work diligently to explore your networks and find and exfiltrate your sensitive data.

Of course, the cloud mobile world is tied directly to the explosion in wireless and mobile devices. Most employees expect to access enterprise resources from their mobile devices, and organizations often don't have the policies and security controls in place to put the guard rails on this access.

Alternately, the cloud has also created many dangerous temptations. Many employees on authorized corporate platforms, reach out to cloud applications that may run afoul of compliance requirements, let alone fail to adequately protect confidential data. Yet the enterprise has no visibility to any of this.

CASB+ is tailor made to address the security challenges with the cloud mobile digital transformation. Let us look at how CASB+ can help.

Integrate with the cloud mobile world. CASB+ provides all of the integrations you need to share information between systems using native application program interfaces (APIs). This consolidation reduced the extreme complexity of trying to use multiple security solutions. You can consistently administer policies across the cloud and other platforms.

Visibility gives you control. CASB+ enables you to see and log all activity to your authorized clouds. This gives you the data you need to support compliance, better secure sensitive data, and shut down access to malicious and/or anomalous activity. Most important, you have visibility of potentially unauthorized and out-of-policy activity that places your organization at risk.

Cloud Data loss prevention (DLP) - integrate or stand alone. Cloud DLP is essential to prevent the leak of sensitive data, either through CASB+ provides one consistent DLP interface that you can use across the broad variety of clouds you deploy. Even your custom applications. Yet you can also integrate CASB+ with your existing enterprise DLP products so that policies can be applied in a uniform way across your enterprise. Most important, with out-of-policy behavior comes an ability to revoke content access at any time. This may be critical to prevent a potential data breach.

Zero Trust encryption has displaced basic "at rest" encryption. First generation CASB solutions with "at rest" encryption are no longer enough for protecting your clouds. Attackers have successfully breached the APIs that have enabled them to compromise even encrypted cloud data. CASB+ brings a comprehensive encryption solution that protects data "at rest," in network transit, in the cloud application layers (API, middleware, memory), and in use. Data encryption keys are strictly retained by you, not shared in the cloud. Most important is that CASB+ enables single key management and policy for all of your cloud applications with uniform controls and a consistent approach.

Detect and defeat malware and malicious attackers faster. CASB+ includes integrated advanced threat feed data which is used by the CASB+ engine to detect and shut down malware quickly. You can leverage your existing security ecosystem to optimize response so this can happen quickly. Technologies like user experience behavior analysis (UEBA) and advanced access control (AAC)

can determine anomalous behavior by a user with valid credentials and shut them down. For example, the download of gigabytes of files at 2 am, or perhaps attempting a valid log-in from Beijing only two hours after logging in from Chicago, Illinois.

SAML integration and single sign-on (SSO). CASB+ provides full support for SSO integration to streamline and protect authentication, and to maintain comprehensive logging of user access.

In summary, CASB+ technology gives you the strong security you need to support the cloud mobile digital transformation. CASB+ will help you reduce expense, cumbersome administration of multiple and disparate security stacks, and substantially improve your user experience.

Centralized administration, ease-of-use, and powerful best-in-class functional capabilities make CASB+ an important choice for your enterprise.

CASB+ is a foundation for SASE

Gartner has recently introduced a new cloud architecture, Secure Access Service Edge (SASE), pronounced 'sassy'. SASE is the future of cloud architecture, solving the complexity of siloed security infrastructure, policies, and measures that are currently divided between on-premises security, legacy solutions, and cloud security. While this concept is not new, until SASE, the closest architecture that discussed continuity between on-premises security and cloud has been the Zero Trust Framework by Forrester. The difference with SASE is it proposes an architecture that we can see taking shape today. Starting with Cloud Access Security Brokers, Software-Defined WANs, Virtual Private Networks as a Service, Firewalls as a Service, Secure Web Gateways, Cloud DNS Services, and Software Defined Perimeter solutions, it is clear we are in a cloud first security environment. The only on-premises solutions left are either for unique security measures that are industry specific, i.e. governments, and very large organizations that require hybrid deployment for the foreseeable future.

CASB+ is focused on replicating the kitchen sink of on-prem security, rearchitected for scale, advanced functionality, centralized management, and ease of operations, to provide organizations the right solutions to maintain full visibility of users and data, protection against zero-days, ransomware, data breaches, malicious insiders, and protection of data at rest and in motion. However, the power of CASB+ comes in its ability to integrate with enterprise applications and legacy solutions allowing customers to extend their investment of on premises solutions such as endpoint and network DLP, integrate with new cloud focused architectures, such as SD-WAN and IAM/SSO solutions, and help operationalize security and specifically cloud security through integrations with SOC applications for SEIMs, EDR, threat hunting, UEBA, and more.

About CipherCloud

CipherCloud, a leader in cloud security, provides powerful end-to-end protection for data resident in the cloud. Our award-winning cloud access security broker delivers comprehensive visibility, data security, threat protection, and compliance for cloud-based assets. Uniquely, CipherCloud provides the deepest levels of data protection and real-time data access control to provide an immediate solution for challenging cloud security and compliance problems. The world's largest global enterprises and government institutions in over 25 countries protect and secure their cloud information with CipherCloud.

To find out more about CipherCloud please go to www.ciphercloud.com.

About the Author

Salah is a seasoned marketing executive with 20+ years of experience in cybersecurity, networking, in enterprise and SMB markets. Currently, Salah is the VP of Marketing at CipherCloud and responsible for product marketing and growth marketing. Most recently he headed up enterprise security product marketing efforts at Symantec for 10+ product lines with global responsibility. Previous to Symantec, Salah has held marketing leadership or dual product & marketing leadership roles at companies such as Cisco, Aruba, and NETGEAR. He has a passion security, for taking innovative products to market and helping companies accelerate growth at any stage.

XOTIC®

Enterprise or System Integrators Thinking Post-Quantum Encryption?

Test it Today! Available at RSA

RSA Conference 2020
San Francisco | February 24 – 28 | Moscone Center

BOOTH 2431
SOUTH HALL

Secure Channels' ultra-light weight, post-quantum XOTIC cryptosystem is now available as a limited-use trial SDK in our booth at RSA and Oracle Marketplace.

PERFECT FOR ENTERPRISE PROCESSES AND DEVELOPING THIRD-PARTY SOFTWARE, XOTIC DELIVERS:

- Scalable one-time pad security
- 512- to beyond 8,000-bit key lengths
- High encryption efficiency
- Cryptosystem encryption is stronger, faster, and lighter-weight than existing standardized encryption algorithms

"We do not foresee the brute-force search to become a threat of any practical importance, even when the dial is in minimum."

– Cryptographers Dr. Alex Biryukov & Dr. Léo Perrin

"In order to break the XOTIC cipher attackers would need insurmountable computing power which nobody will be able to demonstrate in our life time or come up with new, effective attacking methods which nobody has demonstrated to be close to having at this point of time."

– Cryptographers Dr. Lars R. Knudsen & Dr. Bart Preneel

SECURE CHANNELS

www.securechannels.com
contact **sales@securechannels.com**

Demystifying Network Investigations with Packet Data

By Michael Morris, Director of Global Technologies Alliances and Business Development, Endace

A common challenge for security analysts, network operations and applications teams is lacking the right data to troubleshoot security or performance issues quickly and conclusively. Typically, analysts are overloaded with alerts. They need to find ways to reduce the noise and identify the root cause of issues more efficiently.

Investigations often start with log data or network metadata. But this data often doesn't provide enough detail to see exactly what happened or only provides a limited view of activity for a specific user, IP address, application or server. Log data doesn't provide broader insight into related activity and also may potentially be manipulated by malicious actors covering their tracks. Network metadata can provide broader insight, but lacks the detail needed for full event reconstruction.

This lack of concrete, definitive evidence slows issue investigation, resulting in stressed employees and unexamined issues that represent an unknown risk to the organization. Recording full packet data offers a potential solution. Packets hold clues that can be vital for investigating and resolving issues, providing comprehensive evidence across an entire IT environment that can definitively identify lateral movement or command and control traffic, and enable the accurate reconstruction of exfiltrated data.

With today's regulatory environment increasingly requiring mandatory breach notification, relying on log data and metadata alone for investigating security issues doesn't cut it any longer. Packet capture is the only way to be sure you have the data necessary to understand the full depth and breadth of a breach.

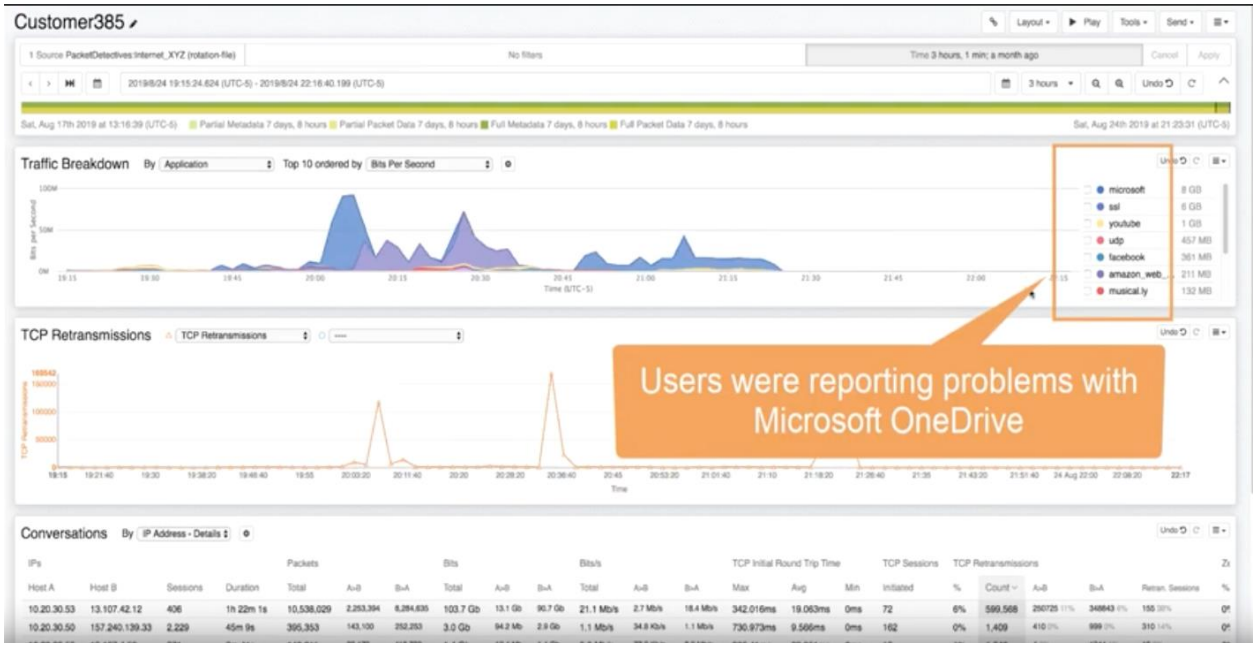
Packet capture solutions can be integrated with SIEMS, IDS, NPMs/APMs and AI technologies (such as Cisco, IBM, Palo Alto Networks, Splunk and many others) making it easy to locate packets of interest. SecOps, NetOps or DevOps analysts can quickly pivot from alerts in their tools directly to the relevant packet data with a single click, making locating suspect packets inside petabytes of network traffic easy. Once the packets have been located, built-in packet decodes in tools such as Wireshark provide a wealth of useful information for analysts.

Let's take a look at a typical investigation example. In this case, it's an application performance issue that's being investigated, but the same workflow can be used to investigate security alerts, hunt for threats or reconstruct exfiltrated data from a security breach.

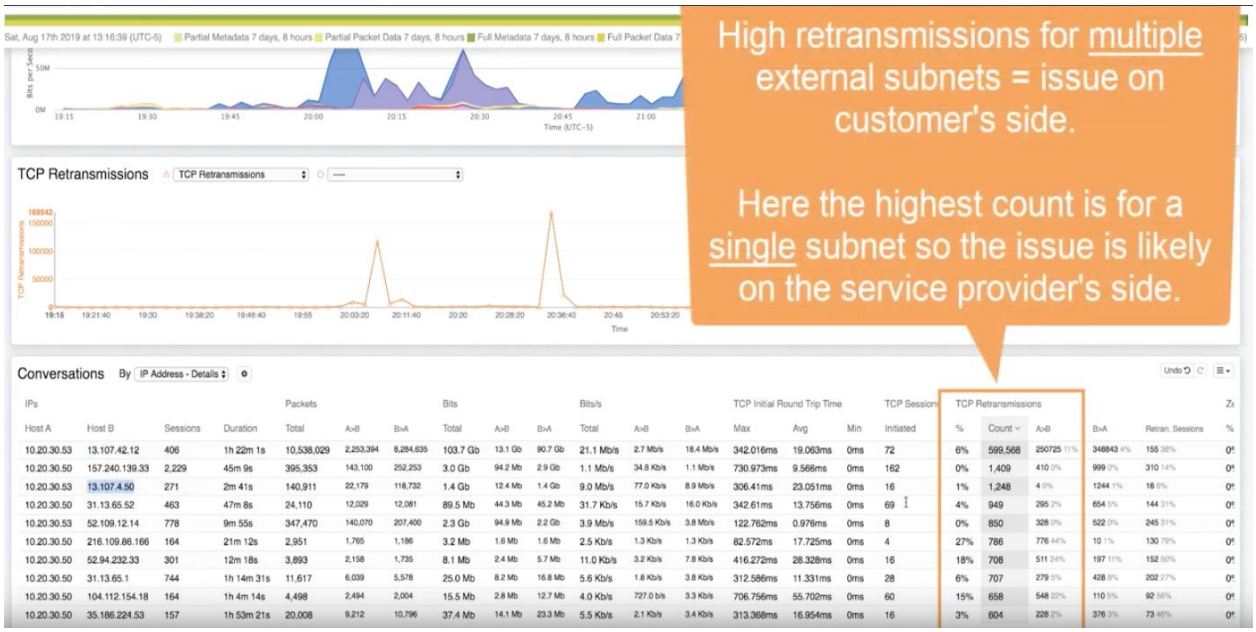
The Case of the Retransmissions

Betty DuBois is an industry-renowned SharkFest educator and network investigator who has created a video that demonstrates how easy investigations can be if you have access to full packet data. Let's walk through how, in just a couple of minutes, you can resolve two specific issues to address in an application performance degradation that generated tickets and alarms due to due to customer complaints.

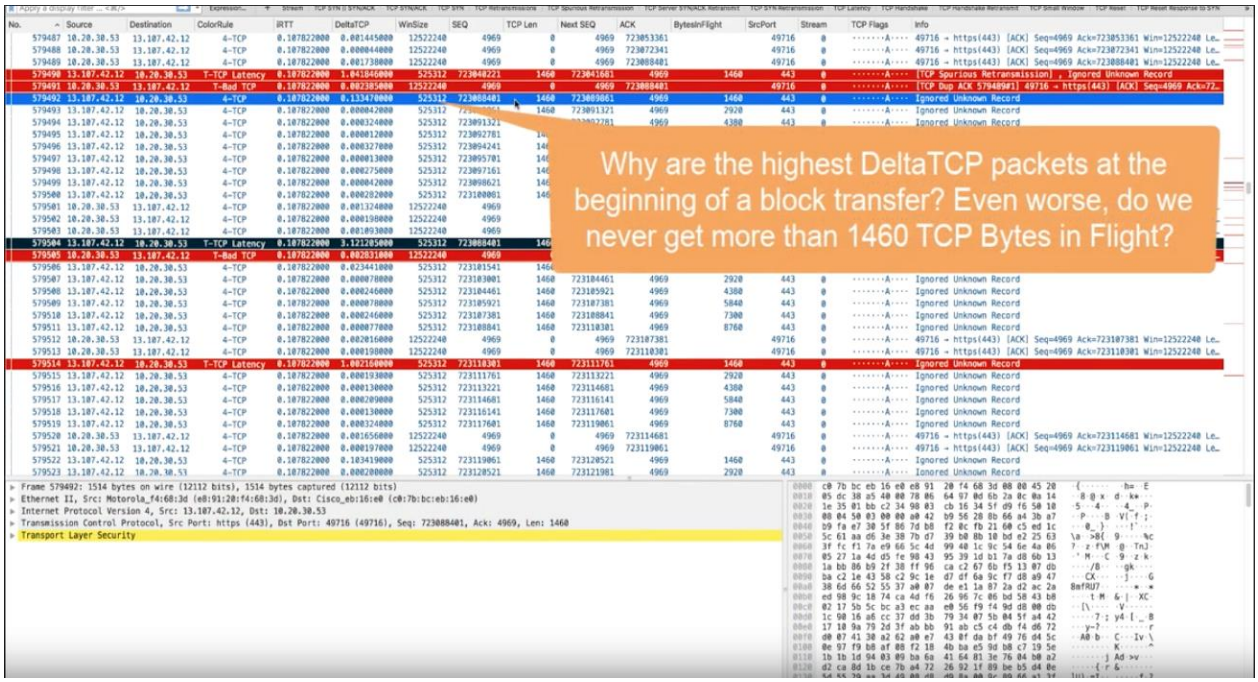
She starts by zooming in on recorded traffic using the time, application, and client IP of impacted users based on reported event tickets. (Time 00:36)



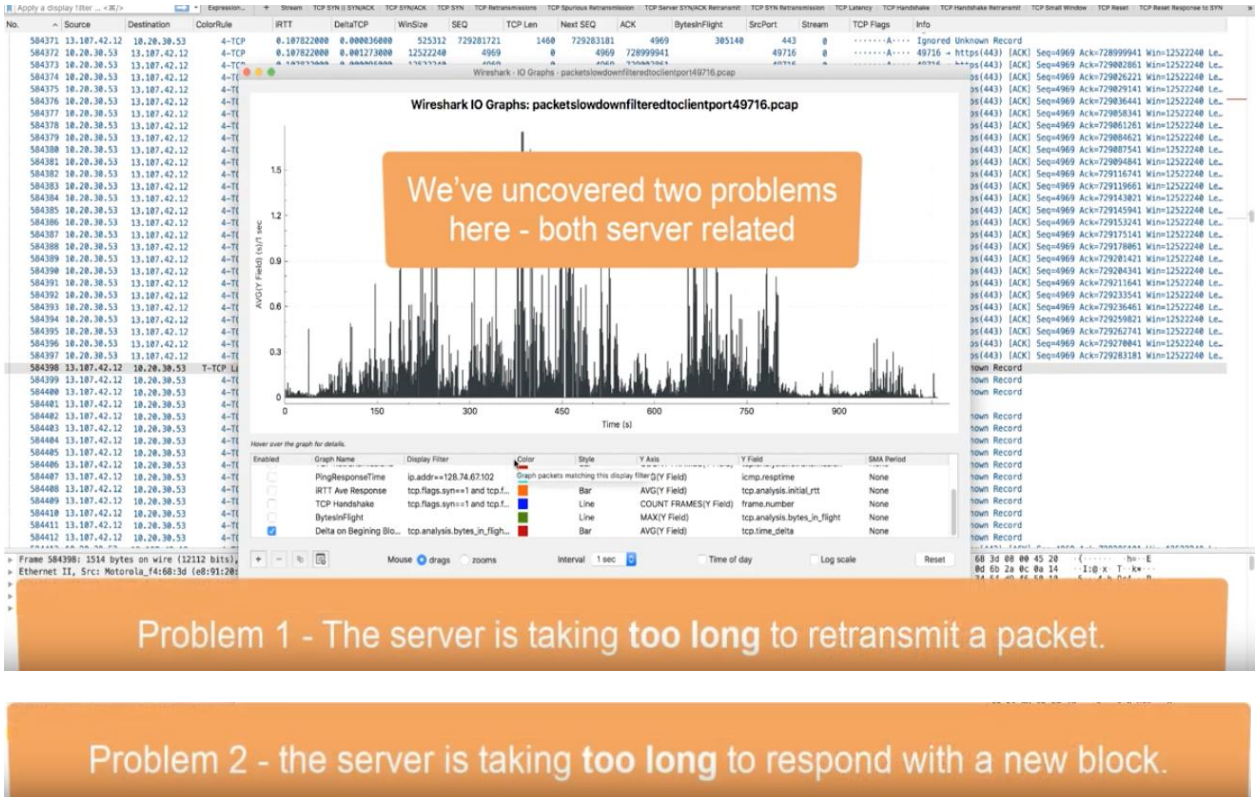
Examining the filtered traffic uncovers unusually high retransmission counts for MS OneDrive traffic – which could be part of the cause. Retransmissions are high on a single subnet, indicating a potential issue on the service provider's side. (Time :58)



Drilling into the packet details uncovers lengthy delays for both standard server response packets and retransmissions (Time 2:33)



Further analysis quickly identifies two issues: the service provider's server is taking too long to retransmit packets and way too long to start sending data to the client. (Time 3:45). In just a few clicks, packet data has enabled Betty to precisely pinpoint the root causes of the issue and identify who is responsible for resolving them – in this case the service provider.



This example demonstrates how access to full packet data can accelerate the process of isolating, investigating and remediating IT issues and security threats with 100% confidence. For the full video, visit *Packet Detectives Episode 1: The Case of the Retransmissions:* (https://blog.endace.com/2019/12/17/demystifying-network-investigations-packet-data-part-1/).

About the Author

Michael Morris is the director of global technologies alliances and business development at Endace. He has more than 20 years of experience in software and hardware solutions for infrastructure and network management and security. Contact: www.Endace.com, sales@endace.com, @endace.

Cross Domain Solutions – Quo Vadis

By Alexander Schellong, VP Global Business, INFODAS

Highly sensitive systems and data assets (domains) are often separated from the Internet or less critical systems. Separation is achieved through isolation, commonly referenced as an air gap. While isolation significantly increases the barrier for data exfiltration or malware infection, Cyberattacks can still happen in various ways. The Stuxnet attack of the Iranian nuclear program is a prominent case in point. However, keeping isolated systems updated with patches or important data and sharing selected data from those systems with others, requires time and manual labor ("swivel chair" or "sneaker" networks). In other words, system and data silos—isolation—contradicts the benefits and needs of digitization such as real-time data sharing in geographically dispersed operating and IT environments.

Accordingly, cross domain solutions (CDS) were developed over the past 10-15 years that allow manual or automatic transfer, access or exchange of data across segmented domains of different classification level. Data can only be shared when necessary and sharing is combined with redaction or validation requirements. CDS are not Firewalls or about encryption.

Outside of military, intelligence, homeland security and some critical infrastructure industry circles many IT professionals are not aware of CDS which also have to adapt to new end-user requirements and technology trends.

What makes Cross Domain Solutions unique?

Most cross domain solutions are accredited by government information security authorities through rigorous multi-year testing. They need to fulfill a complex set of requirements as highly trusted components for the most sensitive environments. This includes security cleared development resources and component supply chain transparency. Moreover, hardware and software security architecture elements such as a hardened operating system, hardware level separation, tamper proof enclosure or enhanced secure logging. CDS functionalities include manual or automatic control of the flow of information between domains, the possibility to add customized filters (parsers) for certain data types or the capability to operate in complex environments (e.g. heat, shock, dust, humidity). Consequently, very few companies have developed CDS and CDS products tend to be higher priced.

Cross Domain Solutions at a glance

Within the Cybersecurity solution market, CDS represent a niche within the data security, DLP and network security space. Currently, CDS are always hardware based solutions (security appliances). Classically CDS are boundary devices that are combined with Firewalls to protect two domains. The domain that needs to be protected or holds more sensitive data is usually referred to as HIGH while the other domain of lesser sensitivity is referred to as LOW.

The most common solution are **data diodes**. They ensure data flow is only possible in one direction which is mostly achieved through the use of hardware of software. To achieve this functionality, the majority of vendors uses a fiber optic cable which leads to galvanic separation between domains similar to the semiconductor of the same name. Within the public sector, data diodes are utilized to provide data to a classified network. In critical infrastructure (e.g. power plants, oil refineries, manufacturing) data diodes are used to send data out of an industrial control network to safeguard its integrity and availability while taking advantage of it for predictive maintenance. Hardware based diodes come in different form factors but many of them are limited in transmission speed or the protocols they support. Some may include pre-defined data filters or malware protection but usually they don't. There are around 30-40 vendors worldwide that offer data diodes.

High Assurance Data Guards (HAG / HADG), Information Exchange Gateways (IEG) or **Security Gateways** are commonly used terms for security appliances that allow for controlled bi-directional data exchange between two domains. Their main purpose is to protect any accidental or purposeful leakage of classified data from a HIGH to a LOW domain. Filters check all data transfers down to the binary level. Some Security Gateways are combined with Firewalls features, optimized for streaming or emailing. There are around 10 vendors worldwide that offer these types of CDS.

Finally, CDS are complemented by solutions to securely **classify data objects**. These can be security appliances, virtual machines or applications. Many applications allow to tag or classify data manually or automatically. Some labels are markings inside documents, some happen through other labels are small external files. Classifications can follow regulatory compliance or a government's classification guidelines (e.g. Confidential, Secret, Top Secret). However, when the label becomes the critical element for downstream release decisions, it needs to be protected against manipulation. In these cases labels are cryptographically bound. There are around 5-6 vendors worldwide that offer government level data classification with secure labels.

Next steps in Cross Domain Solutions

Due to the government accreditation requirements and testing cycles, CDS tend to trail behind technology trends. These government accreditations also create market entry barriers so that vendors can ask for higher prices, even when the technology might already be outdated or offering reduced functionality. Among the areas of CDS that will require improvements are:

- Higher data volumes and lower latency
- Virtual CDS instance (Cloud CDS)
- Improved data discovery and classification (e.g. via Artificial Intelligence)
- Easier deployment
- Easier filters / parsers / Out-of-the-box filters of structured data forats
- Multi-asset management (Dashboard)
- Formfactor miniaturization

Future use-cases might be expanded to other industries within critical infrastructure (e.g. Financial Services) and mobility (e.g. Connected Car, Planes) as the struggle of data custodians and security architects for the right balance between zero trust, protection ("Need to Know") and sharing continues ("Need to Share")

The infodas approach to Cross Domain Solutions

Over 10 years ago infodas was asked by the German military to develop a bi-directional CDS for an IT-service management use-case. Machine data had to be shared from a classified environment with IT service providers such as IBM so that they could monitor and manage the machines without having access to classified data. infodas worked and continues to work closely with the German Federal Office for Information Security BSI to maintain the accreditation status for its products. Now infodas is one of the few vendors in the world that offers products for all CDS scenarios for unidirectional transfer, bi-directional exchange and data classification between HIGH and LOW domains in the SDoT Product Family (Secure Domain Transition). All of the SDoT products feature a unique hardware and software architecture with a microkernel OS following the security by design principle. Fully evaluated and with only 15,000 lines of code the SDoT Microkernel OS differs significantly from secure Linux OS currently used in most trusted CDS on the market.

The SDoT Diode is also the only software based data diode in the world with 9.1 Gbit/s with a NATO, EU and German Secret accreditations. The bi-directional SDoT Security Gateway and Security Gateway Express also gained NATO, EU and German Secret accreditations. UDP, TCP, SMTP/S and HTTP/S can be used for transmission in each 1U 19" rack space appliance without additional proxies. The SDoT Labelling Service can be integrated into most applications to create tamper proof NATO Stanag 4774/8 compliant XML security labels. This makes it easy to integrate the manual classification process in the workflow of whitelisted personnel. The security appliances are used in Navy vessels, weapon systems, data centers or containers around the world.

About the Author

Dr Alexander Schellong, VP Global Business, INFODAS. As a member of the infodas management board, Alexander leads all international activities. He has extensive experience in strategic consulting, business development, general management, business unit leadership and mission critical international project and operations management in Europe, Middle East, Africa and Asia for the U.S. government, German government and other commercial clients. His domain expertise covers among others eGovernment, Cybersecurity, Cloud, BPO or digital transformation. He has authored one book on CRM in the public sector and over 60 articles on a variety of topics at the intersection of technology, society and organizations. He holds a Masters and Phd. He studied and taught at Goethe-University Frankfurt am Main, Harvard Kennedy School, The University of Tokyo and Stanford University.

Alexander can be reached online at a.schellong@infodas.de and @schellong. More information about INFODAS Cybersecurity services and products can be found at http://www.infodas.de

Enterprises Demand MSSPs Offering MDR Services Through Cybersecurity Convergence

By Arun Gandhi, Director of Product Management of the Seceon

Enterprises from all verticals are embracing digital transformation. This new, increasingly connected digital world is bringing tremendous efficiencies to the way we do business. Apart from these advantages, the digital era is also bringing more frequent and aggressive cyber threats. The complex and evolving security landscape, changing IT environment, and the growing compliance requirements have created numerous challenges for organizations. Threat surfaces have broaden significantly and security teams have to defend against sophisticated cyber-attacks, such as, Ransomware, Distributed Denial of Service (DDOS), Inside threats, Vulnerability exploits, Advanced Persistent Threats (APTs), Email phishing, to list few. Cybercrime is rising much faster with the proliferation and adoption of Internet of Things (IoT) and cloud migration. Enterprises are struggling today and will continue to do so in order to acquire the expertise to assist in managing the constantly evolving security threats, and to fully integrate and implement the plethora of security tools that their security teams have acquired. As a result, organizations are turning to Managed Security Service Providers (MSSP) to deliver spectrum of security capabilities and expertise for detecting and responding to cyberattacks.

According to IDC MSSP Survey 2018, global Managed Security Services revenue will grow to 32 Billion USD by 2022 from 22B in 2018 with 10.2% Cumulative Annual Growth Rate (CAGR). As a MSSP, are you well positioned to reap the benefits of this tremendous growth opportunity or still holding on to age-old technology stack and methods that is holding your true potential?

Trends in Cybersecurity

Here are most important cybersecurity trends that are keeping the enterprise Chief Information Security Officers (CISO) up at night and are fueling the growth of Managed Security Services business:

- Sophistication of cyber miscreants growing rapidly. Criminals are leveraging most advanced Artificial Intelligence techniques to identify the most vulnerable enterprises. Therefore, organizations that have their detection and protection methods still stuck in log and rule based methods are no longer safe.

- Proliferation of security tool sets and silos, collectively generate over 100 thousand alerts per day, with major percentage of being false positives.
- Growing Number of Devices and Environments to protect as enterprises are embracing cloud, mobile-first technologies.
- Death of Perimeter as we know it, as employees are more global and mobile and enterprises embracing SaaS (Software-as-a-Service) applications.
- Scarcity of qualified information security professionals. According to Cybersecurity Ventures 2018 report, there will be more 3.5 Million unfilled Cybersecurity jobs globally by 2021.
- Continued growth of Compliance regulations. Privacy and security protection laws are becoming stricter and violation fines levied are growing rapidly.
- Cybercrime as a Service is making it easy for criminals to launch cyber-attacks on organizations and individuals with little effort and knowledge.

How Managed Security Services (MSS) offered today?

Most of the Managed Security Service offerings today, including those offered by very large providers, predicated on the following:

- Log Management: Involving Monitoring, Scanning and Alerting
- Heavy Manual process for Alert/Event investigation with additional retainer fees per incident.
- Defined Network Perimeter that doesn't consider today's changing infrastructure

Challenges with the Traditional Model

The traditional model may have worked when organizations have defined perimeter, limited applications, simple network infrastructure and endpoints. However, it breaks completely with today's rapidly evolving enterprises that are undergoing digital transformations and the increased sophistication of cybercriminals. Here are some of the reasons why:

- Broader attack surface that comprises of not only firewalls, but also SaaS/Cloud infrastructure, Mobile endpoints, email phishing and global workforce.
- Increased volume of data to manage that require Big Data Storage and Analytics.
- Increased volume of known & unknown threats with more than 100M new malware discovered every year. Static Rule and signature based methods no longer work.
- Manual processes no longer efficient for Alert/Event correlation & investigation with hundreds of thousands of security alerts per day reported by multitude of applications.

Next Generation Managed Security Services (MSSP 2.0)

To address evolving enterprise Cybersecurity needs and their demands, MSSPs have recognized need to shift their strategy to:

- Move focus from Alert Notification to Response and Remediation (MDR)
- Moving from Reactive to Proactive Security (AI Assisted SOC).

- Move to more value added services for managing the risk and compliance (Continuous Compliance) vs. just focusing on log aggregation, monitoring and alerting.

And this MSSP 2.0 shift is not only driven to cope with evolving cybersecurity trends, but also are largely driven by:

- Enterprise Digital Transformation
- New IT Architectures
- Cloud & Hybrid-Cloud infrastructures
- New Technology Adoption

aiMSSP: Enabling MSSP 2.0 Shift with aiSIEM, aiMDR and aiSOC

Seceon aiMSSP™ is modern, advanced and fully automated end-to-end multi-tenant platform that is built from ground up to enable service providers to fully embrace MSSP 2.0 shift. aiMSSP™ combines the power of our award winging aiSIEM™ with Multi-Tier, Multi-Tenancy functionality allowing MSSPs to custom package tiers of modern MSS and MDR services to Large, Medium and Small Enterprises and businesses. With integrated, SIEM (Security Information and Event Management), automatic threat detection, containment and remediation, Service providers enjoy the benefits of most advanced Artificial Intelligence (AI) assisted Security Operation Center (aiSOC™), with improved efficiency and effectiveness.

Seceon aiMSSP™ Technology stack offers MSSPs following differentiated capabilities demanded by new age enterprises compared to the traditional stack:

- Machine Learning / Artificial Intelligence
- Big Data and Analytics
- User Behavioral Analytics
- Real-time Threat Intelligence
- Automatic Threat Analysis and Correlation
- Proactive Threat Detection and Hunting
- Netflow Analysis

By embracing aiMSSP™ platform, MSSPs will enjoy the following key benefits:

- Multi-Tier Multi-Tenancy, supports service providers to with shared services technology stack offering end-to-end data separation, threat detection and response, and accelerates revenue generation from new customers. The robust multi-tenancy with multi-tier capability allows MSSPs grow in size quickly and become Master MSSPs.
- An end-to-end Artificial Intelligence driven Managed Detection and Response (aiMDR™) stack in a single platform. Eliminating need to integrate multitude of products to deliver MDR service, powering MSSPs to have fully functional MDR stack up and running in days rather than months and years so they can focus on revenue generation activity rather than spending on Research and Development (R&D).

- With automatic threat detection & correlation through Seceon's innovating dynamic threat models, and automated threat containment and elimination, MSSPs will have AI assisted SOC (aiSOC™) working for them 24/7.

According to Grigoriy Millis, Chief Technology Officer of a global technology provider for 800+ customers with $1 trillion of AUM, "When we did a side-by-side comparison between Seceon and some of the other solutions from larger providers, Seceon was able to detect real-life security threats that the other platforms did not detect. Leveraging Seceon's aiMSSP solution, we are now processing more than over a billion events per day with less than one percent rate of false positives and have increased the efficiency of our IT and SOC personnel by over 77%."

Comparing Traditional MSSP stacks with aiMSSP™ Platform:

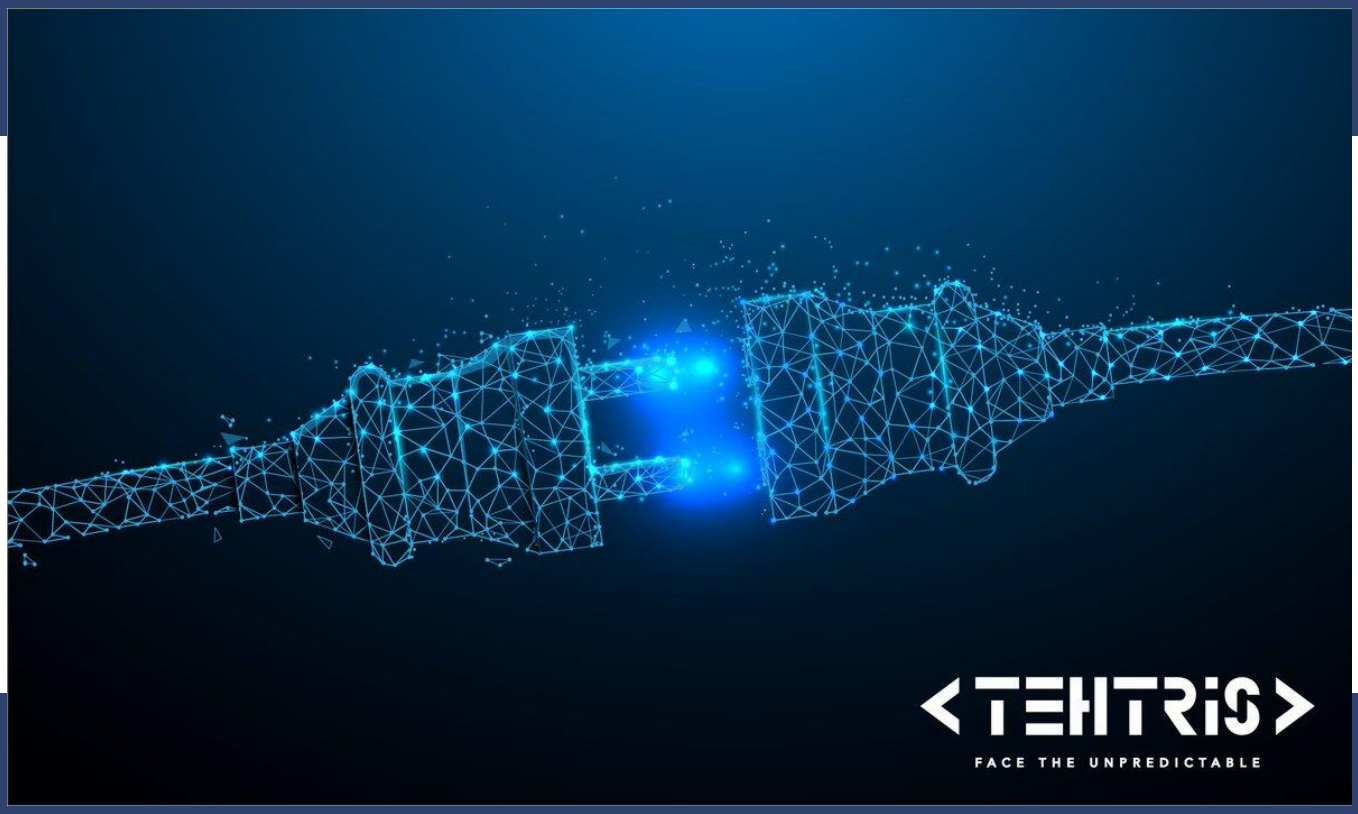
Here is brief comparison of features and benefits offered by aiMSSP platform and how differs from the traditional MSSP stack:

	aiMSSP™	Traditional MSSP
Threat Detection & Alerting	Proactive	Reactive
Incident Response	Automatic	Retainer based
Threat Detection Method	AI Driven & NO Rules	Rule based – Operationally Expensive & ineffective
Compliance	Continuous & Actionable	On Demand & Non-actionable
Netflow Analysis	Yes	
User & Entity Behavioral Analytics	Yes	
Threat Intelligence	Real-time & Integrated	Updated Daily and requires subscription
Artificial Intelligence / ML	Yes	
MDR Enabled	Yes	
Multi-Tenant	Yes	
Multi-Tenant, Multi-Tier and Ready for Master-MSSP use case	Yes	

To summarize, there are a number of moving parts that are involved in defending an enterprise from growing cyberattacks. As cyber risk continues to grow, and threats become more intelligent and capable, enterprises will adopt comprehensive platforms that enable them to eliminate the need for siloed threat detection and response solutions which leave gaps in the enterprise security fabric or simply turn to MSSPs to provide the security services. MSSPs will have to provide the flexibility in delivering 24x7 SOC services that are tied uniquely to the client's needs. This includes all MSS and new services being offered by the MSSPs to manage the security operations as a whole that extends beyond traditional managed security solutions. Seceon's aiMSSP platform proactively detect breaches and threats via comprehensive visibility of all assets (users, applications, services, and hosts and their interactions), and automatically contain and eliminate those threats in real-time.

About the Author

Arun Gandhi is the Director of Product Management of the Seceon. He has more than 17 years of experience with startups and global brands in Cybersecurity, Networking and Cloud technologies. His strong experience includes product management, product marketing, business strategy, competitive positioning, high profile customer engagements, sales enablement, positioning of emerging technologies, development & test in the Service Provider and Enterprise Markets. At Seceon, he is responsible for driving strategic go-to-market initiatives, product roadmap, management and marketing, and executive engagements with customers & partners. Prior to Seceon, Arun held various technical and leadership roles at Juniper Networks, NetBrain Technologies, and Misys Plc (now Finastra). He completed Executive Management program from the prestigious Harvard Business School (Cambridge, MA) and holds Master's in Computer Science from University of New Hampshire (Durham, NH). Arun can be reached online at arun.gandhi@seceon.com and at our company website http://www.seceon.com/



TEHTRIS XDR Platform, A Holistic Cybersecurity Solution

By Laurent Oudot, Founder, CEO at TEHTRIS

TEHTRIS is the European cyber security company that has designed and deployed the smart and holistic **TEHTRIS XDR Platform** in more than 50 countries within heterogeneous, international and distributed infrastructures. In 2019, TEHTRIS captured more than 600 billion events and blocked thousands of intrusion attempts, including highly stealth operations.

TEHTRIS has developed its own defensive weapon called **TEHTRIS XDR Platform** to control and improve the IT security of private and public companies against advanced cyber threats such as cyber espionage or cyber sabotage activities.

The design and research of **TEHTRIS XDR Platform** solutions are carried out by TEHTRIS. The platform is completely modular, through a SaaS model. Customers can smartly choose the security bricks to deploy, with a scalability spirit, by opting for Virtual Appliances in the cloud and/or On-Premise. On top of the **TEHTRIS XDR Platform**, Partners can propose services like SOC, MDR, Management, Hunting, Integration / Deployment / Configuration, etc.

Every year, TEHTRIS XDR Platform analyzes billions of cyber security events worldwide, thanks to the expertise of TEHTRIS experts. 100% of the source code is in TEHTRIS' hands and has been designed with advanced robustness.

TEHTRIS XDR Platform meets the expectations of cybersecurity teams by unifying defensive detection (D) and response (R) capabilities that work in all environments and situations (X), with the following multiple modules that can be adapted and linked to any environment in order to focus against known and unknown threats such as but not limited to, cyber spy operations, ransomwares, sabotages, APT, etc.

In order to deliver such a wide and deep technology, TEHTRIS created multiple different modules described below, and a CIO/CISO can smoothly choose and adapt which technology shall be used depending of the maturity of projects and needs.

TEHTRIS EDR [Endpoint Detection & Response] works in real time on workstations and servers to manage unknown threats and perform preventive hunting and defensive analysis operations.

TEHTRIS EPP [Endpoint Protection Platform] detects and protects operating systems against known threats through advanced antivirus scanning and advanced protection features.

TEHTRIS SIEM [Security Information and Event Management] centralizes all security events in a company and analyses the situation using hundreds of security correlations.

TEHTRIS Mobile Security protects fleets of equipment such as Android tablets and phones, to avoid the spread of unwanted applications against the mobile environments, and to track down major configuration issues regarding cybersecurity.

TEHTRIS Deceptive Response simulates fake devices and fake services to detect stealth and suspicious activities (honeypots) early in the phase. By deluding attackers and providing fake assets, it allows to easily detect insiders or even lateral movements by attackers trying to discover the whole infrastructure during a complex attack with APT like spirit.

TEHTRIS NTA [Network Traffic Analysis] detects intrusions via network flow analysis thanks to signatures and sharp analysis of flows, and it provides new possibilities to do network forensics analysis to know the list of devices that talked together, and many important related meta data.

TEHTRIS SOC [Security Operations Center] & **TEHTRIS MDR** [Managed Detection & Response] & **TEHTRIS GRC** [Governance Risk Compliance] are services that provide analysis, monitoring, response, leading and support capabilities in all situations.

From operational to decision makers, companies that already benefit from **TEHTRIS XDR** Platform intelligence detect weaknesses faster and better anticipate threats, thanks to many activities such as:

- Improved system security and reduced attack surface

- Follow-up of known or unknown offensives from their first appearance

- Hunting campaigns and sophisticated analyses

- Response to incidents via neutralization, machine isolation, remediation...

- Post-mortem analysis and simplification of IS rehabilitation, if necessary

Learn more about Laurent at https://tehtris.com/en/home/

About the Author

Laurent Oudot is a senior international cybersecurity expert, founder and technical director of TEHTRIS. For more than 20 years, his technical skills were used in very sensitive environments such as the Defense Department of the Atomic Energy Commission, the Ministry of Defense, the United Nations, etc. He participated in many national commissions, trainings and expertise, within organizations such as ANSSI or for the Prime Minister. He created TEHTRIS in 2010, specialized in the fight against cyber spying and computer sabotage. This company created the holistic solution called TEHTRIS XDR Platform, a defensive cyber arsenal able to protect infrastructures against stealthy, advanced or unknown cyber threats.

Protect Yourself from Threats and Fraud With XTN

By Guido Ronchetti, CTO of XTN Cognitive Security

XTN develops Behavioral-based Fraud and Threat Protection solutions designed to defend digital businesses. Our security solutions are Cognitive, using proprietary AI algorithms. We also employ behavioral biometric analysis, both to guarantee complete user profiling, and to evaluate and block anomalies and threats in real-time.

Our award-winning Cognitive Security Platform®, specialized in behavioral in-app protection, fraud protection, and digital identity areas, provides our customers with the highest level of security and a fast return on investment.

The XTN team, young, eclectic, and highly qualified, is constantly developing our solutions to remain one step ahead of adversaries. XTN is a global company with offices in Italy, the USA, and the UK.

Cognitive Security

In 2014, we selected XTN Cognitive Security as the name for our company. Cognitive Security is at the heart of what we do, and represents the technological approach used in the development of our solution. Our intent was predictive of a phenomenon that spread years later. Our intention was to explain that we transformed human skills into artificial intelligence, creating our solutions. Cognitive Security is the application of artificial intelligence technologies, modeled on human thought processes, to detect security threats. Our experience in cybersecurity has been digitized to offer real-time, autonomous, efficient, scalable, and accurate evaluation flows. Since learning algorithms make it possible for cognitive systems to constantly mine data and knowledge through advanced analytics, our focus is to refine methods and processes continuously, so the system–learns to anticipate threats and generates proactive responses. Our collective experience in cybersecurity is encoded into our products. This enables us to process and analyze huge volumes of data and identify threats impossible for a human to detect.

Behavioral Biometrics

In a world where compliance requirements, reputation protection, UX-based differentiation, and cost reduction are top priorities for the vast majority of businesses, Behavioral Biometrics solutions are gaining traction. Institutions and industry leaders mention them as an effective way to migrate users to modern authentication flows, minimizing friction. Various industries are facing the same need: strongly identifying users and preventing Fraud, affordably and without added complexity.

It is important to clarify that when we talk about Behavioral Biometrics, we don't mean physical biometrics involving innate human characteristics (for example, fingerprints, face, or iris). Behavioral Biometrics is the discipline related to uniquely identifying and measuring patterns in human activities. The potential is to provide a powerful way to prevent identity-related fraud and malware-based or bot attacks. Our behavioral biometrics provides an effective way to improve your security posture without disrupting your users' experience and without hardware requirements.

Our technology provides smart solutions identifying and measuring patterns. Patterns are activities that could be related to a device and how we interact with it, to a geo-location, or to service-related habits (the usual amount in a payment transaction, the day of the week or hour of the day the user usually operates, the functionality often accessed, etc.).

Our Cognitive Security Platform® features Behavioral Biometrics as a central piece for our user-focused analysis. It allow us to continuously evaluate the anomalies in interacting with the service, allowing the required countermeasures to be dynamic, saving the user from unnecessary friction.

We continuously develop smart solutions that are easy to use, impactful, and cost-effective.

Technology fields

Cybersecurity skills, AI, and behavioral analysis allow us to ensure the protection of our customers' digital services and their users through the award-winning Cognitive Security Platform ®, which features in-app protection, fraud protection, and digital identity components.

Behavioral In-app Protection

In-App protection is a security solution implemented within an application to make it more resistant to attacks. When you distribute a security-critical app to consumers or to enterprise users, you want to be sure that no one can attack it. You should deploy technology capable of protecting the app itself and reporting to you if something goes wrong.

Modern In-App Protection should provide three features:

- Multiple threats detection: ranging from malware presence up to misconfiguration of security conditions inside the endpoint. It should provide runtime detection, evaluation, and reporting.
- Behavioral Analysis: It should use to analyze user behavior and detect anomalies.
- Active App Protection: It should provide active and configurable countermeasures within the application that will prevent your app from working under certain conditions. The main functionalities to implement should be obfuscation and encryption in order to protect the app's assets from reverse engineering attempts (even if the app is not running).

Traditional In-App focuses only on the application as an asset extrapolated from the context. What differentiates us is having a comprehensive vision that considers both the user who accesses the service and the service that is used.

Modern threats are not black and white. Recognizing them requires intelligent processes. Reporting is required to trust the effectiveness of the countermeasure.

At XTN, we have designed a Behavioral In-App Protection solution, using AI in the process of threat detection, providing intelligent tools to protect your app-based services.

Digital Identity

Our solutions generate an effective profile of your customers' digital identity using dynamic digital indicators and guaranteeing high levels of security, and a fluid user experience. Digital identity validation relies on different layers through the XTN Cognitive Security Platform®: behavioral biometrics features, endpoint trust, and cryptographic quantities. These layers help us align the authentication mechanism based on endpoint trust or risk eliminating any friction and include continuous behavioral analysis to recognize anomalies.

Fraud protection

The Cognitive Security Platform is a comprehensive fraud protection ecosystem. Our approach is to correlate different layers of analysis to obtain a holistic view used to detect fraudulent events. The platform considers the posture of the endpoint used to access a critical service, the digital identity of the user, and the risk profiling related to the business content of events. Our technology relies on artificial intelligence for accuracy. Our technology combines different needs that are mandatory in the fraud analysis space: Behavioral perspective, awareness of and insight into risk causes, flexibility, and real-time response. We address the challenge of providing visibility about fraud attempts coming from consumer-facing or internal critical services. The financial

sector is one of our reference markets, where limiting payment-related fraud is imperative. Other markets also need this protection. We are working in the automotive industry to protect digital services in the context of Connected Cars.

XTN offers a comprehensive set of solutions, protecting you from fraud and security threats while keeping your digital service easy to manage and transparent to your end user.

Contact us to discover more about what we can do for your business.

To learn more, visit us online at https://xtn-lab.com/

About the Author

Guido Ronchetti is the CTO of XTN Cognitive Security. In its career, he has been involved in designing several security products. In XTN one of its primary aims has been to apply machine learning models to behavioural related security problems.

The Public Cloud. Is It Secure?

GTB Technologies, Inc.

The Data Protection Company

In today's business environment, data is everything.

With data volumes increasing exponentially, the cloud has become the go-to for many companies to store their vital information.

Offloading data storage and management has worked wonders. Firms no longer have to rely on in-house storage components. Furthermore, the organizational and management tools provided by many cloud services are able to significantly streamline operations--often in ways never imagined.

But outsourcing to the cloud has its costs.

The Security Factor

Experts have been arguing out the pros and cons of data security on the cloud for years.

Indeed, the security challenges unique to cloud based data have produced whole new industries such as that of cloud access security brokers (CASBs).

One thing is clear though:

Putting your data on the cloud means trusting an outside party with your most sensitive information, including your trade secrets to customer PII. From a data loss protection perspective, this is a red flag.

To put it bluntly, the cloud is managed by someone who isn't part of your organization. This raises an important question: in a world of cyber threats and heavy IT compliance obligations, how can administrators know their data is secure in someone else's hands?

Protecting Data in and Out of the Cloud

GTB's Smart data protection platforms allows companies to extend their DLP to the cloud.

The GTB model is designed to secure data in *all* its states, whether in motion, on premises, or on a cloud provider.

With GTB's Cloud Data Protect, organizations have complete visibility to data exiting the cloud including the ability to prevent access and / or block unauthorized access.

ACALVIO

Disrupt the Kill Chain with Continuous Security Validation

Feb 2020

Background: The Challenge of Post-Compromise Security

The Cyber Attack Lifecycle (also known as the Cyber Kill Chain) has long been used to describe the stages of an attack commonly used to compromise sensitive assets. Unfortunately, too much emphasis has been placed on the initial exploitation stages, and not enough on the later stages, after initial penetration. As a result, organizations are ill-prepared to establish and operationalize detection and mitigation strategies. Given that "assume breach" is the new mantra, this is a serious shortcoming. CrowdStrike has taken a leadership position in the industry beseeching organizations to re-tool their Technologies, Processes and People to strive towards the 1/10/60 Goal – 1 minute to Detect, 10 minutes to Analyze and 60 minutes to Remediate. For sure, tall goal, but with the right set of technologies and sustained commitment organizations can get to this. Deception Technologies offer a very proven and cost effective technique to provide Continuous Security Validation. The following article outlines approaches whereby Deception can be applied to every step of the MITRE ATT&CK kill chain to deliver Continuous Security Validation and help organizations achieve their 1/10/60 goal.

The MITRE ATT&CK framework that describes the actions an adversary uses after it has penetrated the target organization. The 11 tactic categories within ATT&CK for Enterprise were derived from the later stages (exploit, control, maintain, and execute) of the Kill Chain. This provides a deeper level of granularity in describing what can occur during an intrusion.

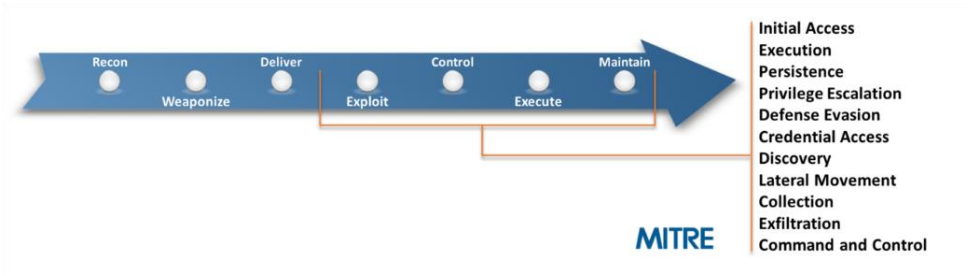


Figure 1:ATT&CK Focuses on Post-Compromise Adversary Tactics

The ATT&CK Framework: Details and Application

ATT&CK was born from research into APT detection research and methodology creation. It consists of three core components:

Highlights

- The MITRE ATT&CK Framework provides a model for understanding adversary post-compromise tactics and techniques.
- ATT&CK is based on the adversary's perspective and is based on real-world malicious activity
- Acalvio ShadowPlex was designed specifically to detect and defeat the tactics documented in ATT&CK.
- ShadowPlex supports defensive strategies for 7 of the 11 adversarial tactics in ATT&CK.
- ShadowPlex operates with minimal false positives and support high-scale enterprise deployment

- **Tactics**: Short-term, tactical adversary goals during an attack. With limited exceptions, they are executed serially, with the ultimate goals being persistence and data exfiltration.
- **Techniques**: Means by which adversaries achieve tactical goals during an attack. Each tactic has a number of techniques attacks can choose from to meet the goal, and there are 219 techniques in total across the 11 tactics.
- **Documented adversary usage of techniques**. These are examples of how actual attacks string together specific techniques to complete the tactics successfully.

A key advantage of ATT&CK is that it is based on "in the wild" research, that is, documented attacker behavior. Another advantage is that it enumerates techniques for Windows, Linux, and MacOS hosts, making it easier to apply based on operating systems in use.

MITRE recommends that ATT&CK be used to architect computer network defenses (CND), using the following methodology:

- Prioritize development and/or acquisition efforts for CND capabilities
- Conduct analyses of alternatives between CND capabilities
- Determine "coverage" of a set of CND capabilities

MITRE also suggests that an organization can continuously evaluate the attack methods it is most susceptible to using threat intelligence, map that to specific techniques, and then implement adequate defenses. Unfortunately, such a nimble approach is beyond the capabilities of most organizations. What is more realistic is to consider deploying technologies and processes proactively to detect and mitigate the most common techniques, narrowing the effort based on the environment. For example, if the initial compromise is almost certainly going to be on network full of Windows hosts, implement detection capabilities for the "Initial Access" and "Exploitation" techniques relevant to Windows only.

Acalvio Support for ATT&CK

Acalvio solutions were designed to meet the challenge of post-compromise detection and response. When evaluated against ATT&CK, Acalvio ShadowPlex provides capabilities relevant to 7 of the 11 tactics in the framework. At a high level, Acalvio delivers

- Fast and accurate incident detection
- Adversary engagement and forensics
- Threat response to retard attack propagation

Like MITRE ATT&CK, Acalvio starts with the premise that attacks will be successful in penetrating the network. ShadowPlex is designed to find these compromises quickly, so that response measures can be executed before persistence and data exfiltration is achieved. It is well understood that most attacks go undetected for weeks or months, allowing the adversary to do significant damage before there is any response or mitigation. It is also well documented that most attacks do leave some form of forensic trail behind – the problem is that these clues are not obvious, and are drowned out in a sea of uncorrelated events and data. Acalvio solves this problem: events detected by ShadowPlex are very likely related to actual attacks, because the platform assets serve no legitimate purpose. This enables the rapid response

essential to execute effective response and mitigation. Implementing Acalvio protects key assets by containing and controlling the attacker early in the exploitation stages of the kill chain.

Acalvio deception-based detection is superior to alternative approaches such as behavioral analytics because it is both more accurate (few false positives) and more efficient and easier to deploy. Furthermore, what separates Acalvio from all other detection solutions is operational efficiency at scale. Legacy "Deception 1.0" honeypot solutions simply cannot be scaled or operated easily. Organizations do not have unlimited budgets for implementing cyber security, and the more efficiently they can deploy funds, the more effectively they can build a robust defensive architecture across their network.

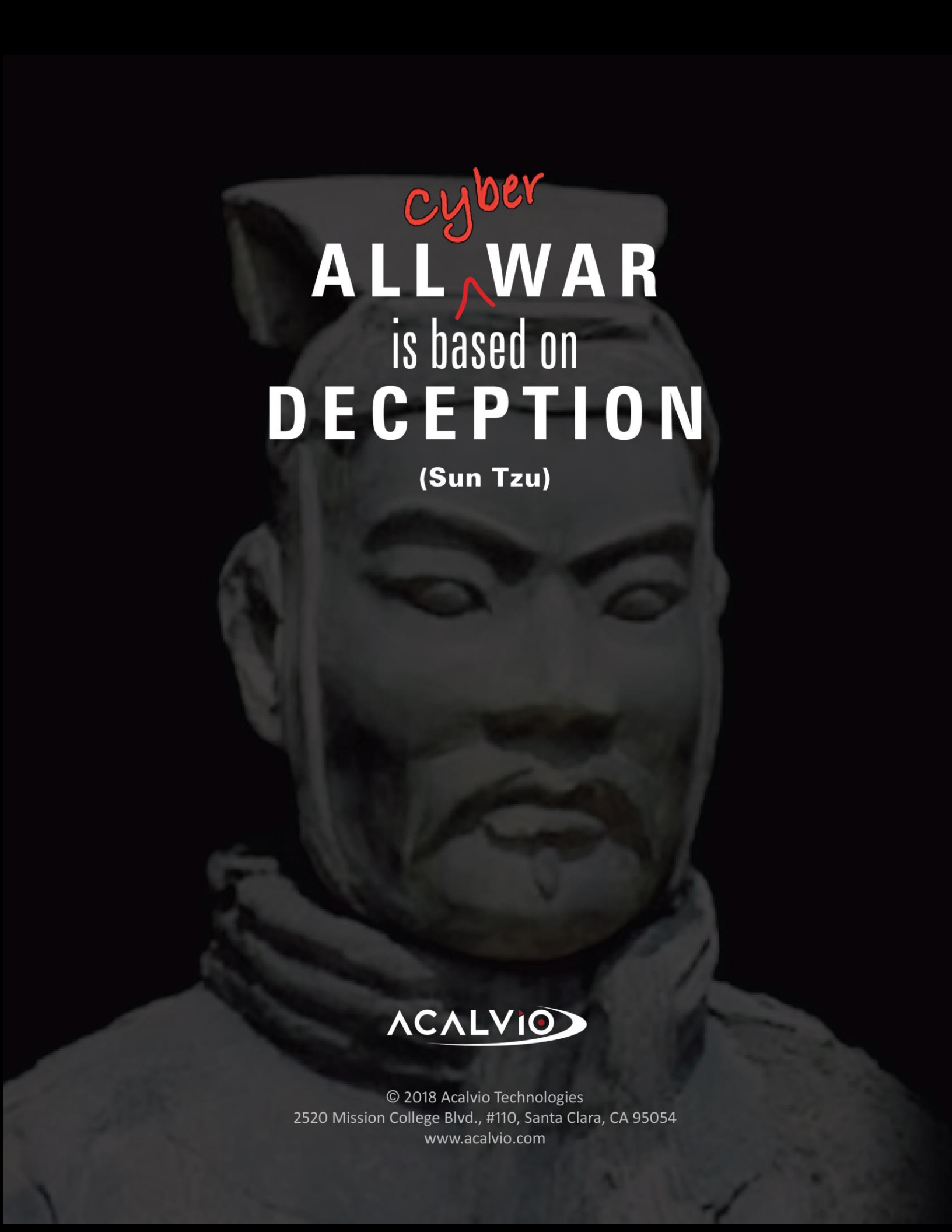
The table below summarizes Acalvio's support for the MITRE ATT&CK framework.

MITRE ATT&CK Tactic	Tactic Description	Acalvio Support
Persistence	Any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.	ShadowPlex Decoys get triggered at the slightest attempt by the adversary in their reconnaissance and discovery efforts. Thereby ShadowPlex detects their attempts to place assets required to persist in the enterprise environment. Lures attract attackers to deception assets, making it easier to detect attempts to establish persistence.
Privilege Escalation	The result of actions that allows an adversary to obtain a higher level of permissions on a system or network. Includes both highly privileged accounts, as well as any account needed for specific objectives during an attack.	ShadowPlex deploys fake privileged accounts in Active Directory as bait (honey tokens) to attract attackers seeking to escalate account privilege.
Defense Evasion	Techniques an adversary may use to evade detection or avoid other defenses. These may be applied at any phase of the overall attack.	ShadowPlex has an AI-based recommendation engine that ensures that the decoys are dynamic and refreshed. Consequently the decoys cannot be fingerprinted and thereby minimizes the possibility of Defenses being evaded.
Credential access	Techniques that result in access to or control over legitimate credentials, typically those with elevated privileges.	Acalvio Distributed Deception deploys decoys and honey tokens that attract attackers. When these assets are accessed using legitimate credentials, the solution identifies those credentials as compromised.
Discovery	Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network.	Discovery includes remote, network-based system discovery. ShadowPlex decoys obscure legitimate targets, and detect attempts by adversaries to discover assets to be compromised. Unlike alternative approaches, Acalvio

		achieves exceptionally low false positive rates.
Lateral Movement	Techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems.	ShadowPlex Fluid Deception deploys advanced decoys across the network, support by breadcrumbs to guide the attacker towards them. Attempts to access these assets provide clear indications of lateral movement activity, while Adversary Behavior Analytics models and records such techniques so that effective response can be quickly achieved.
Collection	Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.	Acalvio baits, or honeytokens, are deployed at scale by ShadowPlex as targets for collection. Attempts to access or copy such baits immediately identifies collection attempts, and the assets being used in the attempt

Summary

In the current cyber threat world that we are faced, there is a fundamental asymmetry – we (the good guys, defenders) need to be right all the time, the attacker (bad guys) need to be right only once. Deception fundamentally changes this asymmetry. Deception, when applied effectively can help organizations disrupt the kill chain, deliver continuous security and help organizations prepare for the 1/10/60 goal [1 minute to Detect, 10 minutes to Investigate and 60 minutes to Remediate].



2520 Mission College Blvd., #110, Santa Clara, CA 95054
www.acalvio.com

Award Winners

Welcome to the Cyber Defense InfoSec Awards for 2020

Cyber Defense Awards in conjunction with Cyber Defense Magazine is pleased to announce the winners of our prestigious annual awards, now in their 8th year, here at the RSA Conference 2020. There are 3,200 cybersecurity companies in the world. Our judges determined that roughly 10-12% deserve this prestigious InfoSec Award for 2020, with a few we will add shortly after the show because we couldn't get all the innovators in print in time - it's exciting to share all these winners at www.cyberdefenseawards.com where the winners list is always up to date.

I've interviewed some of these winners in his www.cyberdefensetv.com hot seat program – where they had to answer difficult and challenging questions – completely unprepared and unscripted. I hope to interview more winners during upcoming Cyber Defense TV opportunities.

In addition, our search focused us on startups and early stage players to find those who could have the potential to stop breaches in a new and innovative way. It, therefore, gives us great pleasure to recognize and celebrate the accomplishments of winners, who have unique people, software, hardware, services and even cloud-based solutions that might just help you get one step ahead of the next cybersecurity threat.

Congratulations to all our winners!

Gary S. Miliefsky, CEO
Cyber Defense Media Group
Publisher, Cyber Defense Magazine

Access Control

ERP Maestro Best Product Access Control

Advanced Persistent Threat (APT) Detection and Response

Cythereal Cutting Edge Advanced Persistent Threat (APT) Detection and Response

Illusive Networks Most Innovative Advanced Persistent Threat (APT) Detection and Response

QI-ANXIN Next Gen Advanced Persistent Threat (APT) Detection and Response

Advanced Threat Detection

Acalvio Technologies Editor's Choice Advanced Threat Detection

Anti-Malware

Ericom Software Most Innovative Anti-Malware
Iboss Market Leader Anti-Malware
Menlo Security Cutting Edge Anti-Malware
PC Matic, Inc. Best Product Anti-Malware

Anti-Phishing

Ericom Software Publisher's Choice Anti-phishing
Inspired eLearning, LLC. Editor's Choice Anti-phishing
Vade Secure Hot Company Anti-phishing

Application Isolation

Microsoft Next Gen Application Isolation

Application Security

Brinqa Editor's Choice Application Security
Checkmarx Hot Company Application Security
Data Theorem Most Promising Application Security
NowSecure Publisher's Choice Application Security
Signal Sciences Editor's Choice Application Security
Veracode Best Product Application Security
WhiteHat Security Cutting Edge Application Security
WhiteSource Most Innovative Application Security
XTN Cognitive Security Market Leader Application Security
Zimperium Next Gen Application Security

Artificial Intelligence and Machine Learning

Cythereal Hot Company Artificial Intelligence and Machine Learning
ExtraHop Cutting Edge Artificial Intelligence and Machine Learning
IRONSCALES Most Innovative Artificial Intelligence and Machine Learning
Silobreaker Next Gen Artificial Intelligence and Machine Learning
Vectra AI Next Gen Artificial Intelligence and Machine Learning
Zimperium Best Product Artificial Intelligence and Machine Learning

Authentication (Multi, Single or Two-Factor)

HID Global Market Leader Authentication (Multi, Single or Two-Factor)
ID.me Publisher's Choice Authentication (Multi, Single or Two-Factor)
Trusona Editor's Choice Authentication (Multi, Single or Two-Factor)

Automated Penetration Testing Tools

Pcysys Most Innovative Automated Penetration Testing Tools

Autonomous Awareness Training

CybeReady Cutting Edge Autonomous Awareness Training

Biometrics

Nuance Communications Most Innovative Biometrics
XTN Cognitive Security Market Leader Biometrics

Breach and Attack Simulation

Cymulate Best Product Breach and Attack Simulation

Central Log Management

Fluency Security Next Gen Central Log Management

Chief Executive Officer of the Year

Keeper Security Publisher's Choice Chief Executive Officer of the Year "Darren Guccione"

CSIOS Corporation Most Innovative Chief Executive Officer of the Year "Mr. Cesar Pie"

Darktrace Next Gen Chief Executive Officer of the Year "Nicole Eagan"

Secure Code Warrior Editor's Choice Chief Executive Officer of the Year "Pieter Danhieux, CEO & Co-founder"

White Ops Editor's Choice Chief Executive Officer of the Year "Tamer Hassan"

Bishop Fox Cutting Edge Chief Executive Officer of the Year "Vinnie Liu"

Cloud Security

AT&T Cybersecurity Hot Company Cloud Security
Attivo Networks Best Product Cloud Security
DivvyCloud Cutting Edge Cloud Security
FireMon Next Gen Cloud Security
Guardicore Market Leader Cloud Security
iStorage Publisher's Choice Cloud Security
Lacework Editor's Choice Cloud Security
McAfee Most Innovative Cloud Security
Netskope Editor's Choice Cloud Security
Threat Stack Inc Cutting Edge Cloud Security
Vectra AI Next Gen Cloud Security
Zscaler Hot Company Cloud Security

Compliance

Darktrace Market Leader Compliance
Inspired eLearning, LLC. Most Innovative Compliance
SaltStack Next Gen Compliance
SCADAfence Cutting Edge Compliance
TrustArc Hot Company Compliance

Consent and Preference Management

OneTrust Best in Class Consent and Preference Management

Cyber Defense InfoSec Awards for 2020

Content Disarm and Reconstruction (CDR)

Sasa Software Most Innovative Content Disarm and Reconstruction (CDR)

Continuous Controls Monitoring

Panaseer Editor's Choice Continuous Controls Monitoring

Critical Infrastructure Protection

Attivo Networks Hot Company Critical Infrastructure Protection
Honeywell Most Innovative Critical Infrastructure Protection
INFODAS Publisher's Choice Critical Infrastructure Protection
SCADAfence Next Gen Critical Infrastructure Protection

Cross Domain Solutions (CDS) for Information Assurance

INFODAS Cutting Edge Cross Domain Solutions (CDS) for Information Assurance

CTO of the Year "Craig Lurey"

Keeper Security Most Innovative CTO of the Year "Craig Lurey"

Cyber Defense Services

THETA432 Cutting Edge Cyber Defense Services

Cyber Defense InfoSec Awards for 2020

Cyber Security Program Management Platform

PlexTrac Market Leader Cyber Security Program Management Platform

Cyber Security Services

THETA432 Hot Company Cyber Security Services

Cyber Strategist of the Year

CSIOS Corporation Next Gen Cyber Strategist of the Year

Cyber Threat Services

THETA432 Publisher's Choice Cyber Threat Services

Cybersecurity Analytics

Awake Security Best Product Cybersecurity Analytics

Cybersecurity Artificial Intelligence

BlackBerry Hot Company Cybersecurity Artificial Intelligence
Darktrace Most Innovative Cybersecurity Artificial Intelligence
Hillstone Networks Next Gen Cybersecurity Artificial Intelligence
Stellar Cyber Editor's Choice Cybersecurity Artificial Intelligence

Cyber Defense InfoSec Awards for 2020

Cybersecurity Conference Series

Semperis Publisher's Choice Cybersecurity Conference Series

Cybersecurity Internet of Things (IoT)

Armis Market Leader Cybersecurity Internet of Things (IoT)

Medigate Hot Company Cybersecurity Internet of Things (IoT)

SAM Seamless Network Most Innovative Cybersecurity Internet of Things (IoT)

Sternum Next Gen Cybersecurity Internet of Things (IoT)

Cybersecurity Mergers & Acquisitions Firm of the Year

America's Growth Capital Market Leader Cybersecurity Mergers & Acquisitions Firm of the Year

Momentum Cybersecurity Group LLC Most Innovative Cybersecurity Mergers & Acquisitions Firm of the Year

Cybersecurity Research

Bishop Fox Cutting Edge Cybersecurity Research

Cybersecurity Service Provider Optimization Services

CSIOS Corporation Next Gen Cybersecurity Service Provider Optimization Services

Cyber Defense InfoSec Awards for 2020

Cybersecurity Startup of the Year

Silverfort Most Promising Cybersecurity Startup of the Year

Cybersecurity Talent Services (Staffing)

Prosyntix LLC Editor's Choice Cybersecurity Talent Services (Staffing)

Cybersecurity Training

Inspired eLearning, LLC. Market Leader Cybersecurity Training
MediaPRO Hot Company Cybersecurity Training
Secure Code Warrior Best Product Cybersecurity Training

Cybersecurity Training for InfoSec Professionals

Infosec Institute Most Innovative Cybersecurity Training for InfoSec Professionals

Cybersecurity Venture Capitalist of the Year

Stony Lonesome Group Hot Company Cybersecurity Venture Capitalist of the Year
"Sean Drake"

AllegisCyber Capital Market Leader Cybersecurity Venture Capitalist of the Year
"Robert R. Ackerman, Jr."

Night Dragon Most Innovative Cybersecurity Venture Capitalist of the Year

"David DeWalt"

Cyber Defense InfoSec Awards for 2020

Cyberspace Operations Team of the Year

CSIOS Corporation Best Product Cyberspace Operations Team of the Year

Data Behavior Analytics

Cyberhaven Cutting Edge Data Behavior Analytics

Data Breach Prevention

Don't Be Breached Market Leader Data Breach Prevention

Data Center Security

ShieldX Cutting Edge Data Center Security

Data Discovery

Ground Labs Next Gen Data Discovery

Data Leakage Protection

DriveLock SE Next Gen Data Leakage Protection

Namogoo Best Product Data Leakage Protection

Data Loss Prevention (DLP)

Altaro Software Next Gen Data Loss Prevention (DLP)

Altitude Networks Publisher's Choice Data Loss Prevention (DLP)

CipherCloud Editor's Choice Data Loss Prevention (DLP)

Clearswift Market Leader Data Loss Prevention (DLP)

CoSoSys Most Innovative Data Loss Prevention (DLP)

Fidelis Cybersecurity Best Product Data Loss Prevention (DLP)

GTB Technologies Cutting Edge Data Loss Prevention (DLP)

Netskope Hot Company Data Loss Prevention (DLP)

Data Rights Management

CipherCloud Market Leader Data Rights Management

Database Security, Data Leakage-Protection/Extrusion Prevention

Don't Be Breached Hot Company Database Security, Data Leakage-Protection/Extrusion Prevention

INFODAS Next Gen Database Security, Data Leakage-Protection/Extrusion Prevention

Cyber Defense InfoSec Awards for 2020

Deception Based Security

Attivo Networks Most Innovative Deception Based Security

Fidelis Cybersecurity Hot Company Deception Based Security

Illusive Networks Next Gen Deception Based Security

Ntrepid LLC Editor's Choice Deception Based Security

Deception Based Threat Detection

Acalvio Technologies Cutting Edge Deception Based Threat Detection

Deep Sea Phishing and Next Generation Email Security

Ericom Software Best Product Deep Sea Phishing and Next Generation Email Security

Defensive Cyberspace Operations Service Provider

CSIOS Corporation Best Product Defensive Cyberspace Operations Service Provider

Cyber Defense InfoSec Awards for 2020

Digital Footprint Security

Ntrepid LLC Publisher's Choice Digital Footprint Security

RiskIQ Most Innovative Digital Footprint Security

ZeroFOX Next Gen Digital Footprint Security

Email Security

BitDam Editor's Choice Email Security

Trustifi Most Innovative Email Security

Email Security and Management

ZeroFOX Hot Company Email Security and Management

Encryption

Fortanix Market Leader Encryption

SafeLogic Publisher's Choice Encryption

Endpoint Detection and Response (EDR)

Sangfor Technologies Inc. Next Gen Endpoint Detection and Response (EDR)

Endpoint Protection Platform of the Year

Cybereason Most Innovative Endpoint Protection Platform of the Year

Endpoint Security

Adaptiva Hot Company Endpoint Security

Allied Telesis Next Gen Endpoint Security

Attivo Networks Cutting Edge Endpoint Security

BufferZone Next Gen Endpoint Security

DataLocker Hot Company Endpoint Security

GTB Technologies Publisher's Choice Endpoint Security

McAfee Endpoint Security 10.7 Most Innovative Endpoint Security

McAfee MVISION EDR 1 Most Scalable Endpoint Security

Microsoft Editor's Choice Endpoint Security

SparkCognition Cutting Edge Endpoint Security

TEHTRIS Publisher's Choice Endpoint Security

VMware Carbon Black Best Product Endpoint Security

WatchGuard Technologies Market Leader Endpoint Security

Enterprise Key Management

Futurex Best Product Enterprise Key Management

Enterprise Mobile Threat Defense

Zimperium Most Innovative Enterprise Mobile Threat Defense

Enterprise Security

Axonius Editor's Choice Enterprise Security

iboss Most Innovative Enterprise Security

Nucleon Next Gen Enterprise Security

SpyCloud Cutting Edge Enterprise Security

TEHTRIS Best Product Enterprise Security

ThreatQuotient Market Leader Enterprise Security

Enterprise Threat Protection

Microsoft Hot Company Enterprise Threat Protection

ERP Security

Onapsis Inc. Best Product ERP Security

Cyber Defense InfoSec Awards for 2020

Fraud Prevention

Kount Publisher's Choice Fraud Prevention

White Ops Most Innovative Fraud Prevention

Go-To-Market Agency for Cyber Security Startups

Forabilis Next Gen Go-To-Market Agency for Cyber Security Startups

Governance, Risk and Compliance

LogicGate Hot Company Governance, Risk and Compliance

OneTrust Market Leader Governance, Risk and Compliance

Healthcare Cybersecurity

Alexio Corporation Cutting Edge Healthcare Cybersecurity

Healthcare IoT Security

Medigate Best Product Healthcare IoT Security

ICS/SCADA Security

Darktrace Best Product ICS/SCADA Security

Honeywell Most Innovative ICS/SCADA Security

Onward Security Corporation Next Gen ICS/SCADA Security

SCADAfence Cutting Edge ICS/SCADA Security

Identity and Access Management

Auth0 Cutting Edge Identity and Access Management

Evident ID Editor's Choice Identity and Access Management

LogMeIn Best Product Identity and Access Management

Saviynt Next Gen Identity and Access Management

Silverfort Most Innovative Identity and Access Management

Simeio Solutions, LLC Market Leader Identity and Access Management

Idaptive Publisher's Choice Identity and Access Management

Identity Proofing and Corroboration

TransUnion Market Leader Identity Proofing and Corroboration

Cyber Defense InfoSec Awards for 2020

Incident Management

OTRS Group Cutting Edge Incident Management

Incident Response

Onward Security Corporation Best Product Incident Response

Siemplify Most Innovative Incident Response

InfoSec Startup of the Year

CyCognito Editor's Choice InfoSec Startup of the Year

PlexTrac Most Innovative InfoSec Startup of the Year

Remediant Next Gen InfoSec Startup of the Year

SaltStack Cutting Edge InfoSec Startup of the Year

Insider Threat Detection

Attivo Networks Next Gen Insider Threat Detection

Code42 Cutting Edge Insider Threat Detection

Darktrace Hot Company Insider Threat Detection

Illusive Networks Editor's Choice Insider Threat Detection

Insider Threat Prevention

Allied Telesis Most Innovative Insider Threat Prevention

Gurucul Best Product Insider Threat Prevention

Internet of Things (IoT) Security

Intrinsic ID Most Innovative Internet of Things (IoT) Security

NCP engineering GmbH Publisher's Choice Internet of Things (IoT) Security

Nodeware Cutting Edge Internet of Things (IoT) Security

Onward Security Corporation Next Gen Internet of Things (IoT) Security

IoT Security

Darktrace Publisher's Choice IoT Security

IT Automation and Cybersecurity

HelpSystems Market Leader IT Automation and Cybersecurity

IT Vendor Risk Management (ITVRM)

OneTrust Best Product IT Vendor Risk Management (ITVRM)

ProcessUnity Next Gen IT Vendor Risk Management (ITVRM)

Keys Management & Protection

AKEYLESS Market Leader Keys Management & Protection

Malware Analysis

ReversingLabs Most Innovative Malware Analysis

Malware Defense Platform with Predictive Artificial Intelligence (A.I.)

Cythereal Most Innovative Malware Defense Platform with Predictive Artificial Intelligence (A.I.)

Malware Detection

Microsoft Best Product Malware Detection

Managed Detection and Response (MDR)

AT&T Cybersecurity Market Leader Managed Detection and Response (MDR)
Confluera Cutting Edge Managed Detection and Response (MDR)
CyberProof Next Gen Managed Detection and Response (MDR)
Microsoft Market Leader Managed Detection and Response (MDR)
QI-ANXIN Most Innovative Managed Detection and Response (MDR)

Managed Prevention, Detection and Response Services (MPDRS)

THETA432 Next Gen Managed Prevention, Detection and Response Services (MPDRS)

Managed Security Service Provider (MSSP)

Infinite Group, Inc. Editor's Choice Managed Security Service Provider (MSSP)

Seceon, Inc. Publisher's Choice Managed Security Service Provider (MSSP)

Messaging Security

Wire Best Product Messaging Security

Mobile Endpoint Security

Zimperium Best Product Mobile Endpoint Security

Mobile Privacy Expert of the Year "Michael Nash"

Privacy Research Inc. Most Innovative Mobile Privacy Expert of the Year "Michael Nash"

Multi-factor Authentication

WatchGuard Technologies Market Leader Multi-factor Authentication

Network Detection and Response

ExtraHop Cutting Edge Network Detection and Response

Network Security and Management

Corelight Cutting Edge Network Security and Management

Endace Most Innovative Network Security and Management

Gigamon Market Leader Network Security and Management

Keysight Technologies Next Gen Network Security and Management

Verodin Best Product Network Security and Management

Zero Networks Editor's Choice Network Security and Management

Network Traffic Analysis

Fidelis Cybersecurity Most Innovative Network Traffic Analysis

Operational Technology (OT) & Industrial Control Systems (ICS) Cybersecurity

Sasa Software Cutting Edge Operational Technology (OT) & Industrial Control Systems (ICS) Cybersecurity

Operational Technology (OT) & Internet of Things (IoT) Cybersecurity

Nozomi Networks Market Leader Operational Technology (OT) & Internet of Things (IoT) Cybersecurity

Packet Capture Platform

Endace Best Product Packet Capture Platform

Password Management

Keeper Security Best Product Password Management

Patch and Configuration Management

Ivanti Most Innovative Patch and Configuration Management

SaltStack Best Product Patch and Configuration Management

Privacy Management Software

WireWheel Next Gen Privacy Management Software

Cyber Defense InfoSec Awards for 2020

Privileged Account Security

Centrify Corporation Cutting Edge Privileged Account Security
CyberArk Market Leader Privileged Account Security
Hysolate Best Product Privileged Account Security
Remediant Hot Company Privileged Account Security
Thycotic Next Gen Privileged Account Security

Public Relations Team for InfoSec Companies

Madison Alexander PR Best in Class Public Relations Team for InfoSec Companies

Purple Teaming Platform

PlexTrac Most Innovative Purple Teaming Platform

Ransomware Recovery Solution

Semperis Cutting Edge Ransomware Recovery Solution

Risk Management

AccessIT Group Publisher's Choice Risk Management
Brinqa Best Product Risk Management
Digital Shadows Next Gen Risk Management
SecurityScorecard Hot Company Risk Management
The Chertoff Group Editor's Choice Risk Management
WootCloud Inc Most Innovative Risk Management

SaaS/Cloud Security

CyCognito Best Product SaaS/Cloud Security
Darktrace Cutting Edge SaaS/Cloud Security
GTB Technologies Next Gen SaaS/Cloud Security
iboss Market Leader SaaS/Cloud Security
ManagedMethods Publisher's Choice SaaS/Cloud Security
Menlo Security Editor's Choice SaaS/Cloud Security
Nodeware Most Innovative SaaS/Cloud Security
Spin Technology, Inc. Editor's Choice SaaS/Cloud Security
ThreatBook Cutting Edge SaaS/Cloud Security
Zscaler Publisher's Choice SaaS/Cloud Security

Secrets Management and Protection

AKEYLESS Next Gen Secrets Management and Protection

Security Abstraction

FireMon Most Innovative Security Abstraction

Security Awareness CBT

KnowBe4 Market Leader Security Awareness CBT

Security Awareness Training for Employees

Infosec Institute Best Product Security Awareness Training for Employees

Security Company of the Year

Bishop Fox Hot Security Company of the Year

BlackBerry Best Security Company of the Year

CyCognito Cutting Edge Security Company of the Year

Darktrace Next Gen Security Company of the Year

DivvyCloud Market Leader Security Company of the Year

Hillstone Networks Publisher's Choice Security Company of the Year

iboss Editor's Choice Security Company of the Year

IGI Most Innovative Security Company of the Year

INFODAS Editor's Choice Security Company of the Year

ReversingLabs Cutting Edge Security Company of the Year

Secure Code Warrior Publisher's Choice Security Company of the Year

SecurityScorecard Next Gen Security Company of the Year

WatchGuard Technologies Hot Company Security Company of the Year

Security Detection and Response Operation Platform

Yuanhe Technology Co., Ltd. Most Innovative Security Detection and Response Operation Platform

Cyber Defense InfoSec Awards for 2020

Security Information Event Management (SIEM)

Devo Technology, Inc. Editor's Choice Security Information Event Management (SIEM)

Empow Cutting Edge Security Information Event Management (SIEM)

LogRhythm Best Product Security Information Event Management (SIEM)

Seceon, Inc. Next Gen Security Information Event Management (SIEM)

Securonix Market Leader Security Information Event Management (SIEM)

Security Investigation Platform

Endace Hot Company Security Investigation Platform

ThreatQuotient Cutting Edge Security Investigation Platform

Security Project of the Year

Cybereason Best Product Security Project of the Year

Security Ratings

SecurityScorecard Best Product Security Ratings

Security Team of the Year

GroupSense Most Innovative Security Team of the Year

IGI Market Leader Security Team of the Year

Security Training

Inspired eLearning, LLC. Hot Company Security Training
Security Mentor, Inc. Cutting Edge Security Training

Small to Medium Size Business (SMB) Cybersecurity

Defendify Most Innovative Small to Medium Size Business (SMB) Cybersecurity
Keeper Security Best Product Small to Medium Size Business (SMB) Cybersecurity
Nodeware Next Gen Small to Medium Size Business (SMB) Cybersecurity
Untangle Most Innovative Small to Medium Size Business (SMB) Cybersecurity

SOC-as-a-Service

Proficio Best Product SOC-as-a-Service

Storage and Archiving

DataLocker Cutting Edge Storage and Archiving

Third Party Risk Management (TPRM)

CyberGRX Publisher's Choice Third Party Risk Management (TPRM)
Panorays Most Innovative Third Party Risk Management (TPRM)
ProcessUnity Next Gen Third Party Risk Management (TPRM)
SecurityScorecard Editor's Choice Third Party Risk Management (TPRM)

Cyber Defense InfoSec Awards for 2020

Threat and Vulnerability Management

Microsoft Most Innovative Threat and Vulnerability Management

Threat Hunting

Acalvio Technologies Hot Company Threat Hunting

Threat Intelligence

DomainTools Cutting Edge Threat Intelligence
EclecticIQ Editor's Choice Threat Intelligence
KELA Cutting Edge Threat Intelligence
Nucleon Next Gen Threat Intelligence
Recorded Future Market Leader Threat Intelligence
Resecurity Publisher's Choice Threat Intelligence
Silobreaker Editor's Choice Threat Intelligence
Terbium Labs Most Innovative Threat Intelligence
ThreatBook Best Product Threat Intelligence
ThreatQuotient Hot Company Threat Intelligence

Transportation Cybersecurity

Cervello Most Innovative Transportation Cybersecurity

Unified Endpoint Management (UEM)

ManageEngine Next Gen Unified Endpoint Management (UEM)

Cyber Defense InfoSec Awards for 2020

Unified Threat Management (UTM)

WatchGuard Technologies Best Product Unified Threat Management (UTM)

User Behavior Analytics

LinkShadow Cutting Edge User Behavior Analytics

LogRhythm Market Leader User Behavior Analytics

vCISO Program of the Year "Andrew Hoyen"

IGI Best Product vCISO Program of the Year "Andrew Hoyen"

Vulnerability Assessment, Remediation, and Management

PlexTrac Hot Company Vulnerability Assessment, Remediation, and Management

SaltStack Most Innovative Vulnerability Assessment, Remediation, and Management

Vulnerability Management

Brinqa Cutting Edge Vulnerability Management

Kenna Security Most Innovative Vulnerability Management

Nodeware Hot Company Vulnerability Management

Onward Security Corporation Best Product Vulnerability Management

Web Application Security

ThreatX Next Gen Web Application Security

Women in Cybersecurity

Alexio Corporation Most Innovative Women in Cybersecurity "Anne Genge"

ThreatQuotient Cutting Edge Women in Cybersecurity "Gigi Schumm"

Cyberhaven Next Gen Women in Cybersecurity "Liron Pergament-Gal"

***

These women exemplify why we will be including them in the larger 2020 Women in Cybersecurity list as we get closer to our Black Unicorn Awards in August.

Here's last year's list to add these women to:

https://cyberdefenseawards.com/top-25-women-in-cybersecurity/

HERJAVEC GROUP

Celebrating Over 15 Years of Cybersecurity Operations Excellence

At Herjavec Group, information security is what we do.

You may know me from making deals on television, but my passion lies in innovating technology - yes, cybersecurity.

Over 15 years ago we started the business selling commercial firewalls to IT buyers. Over time we've seen a monumental shift towards what we are all familiar with - the cybercrime epidemic. Now our customers are challenged to address compliance requirements, incident response plans, nation state threats, security awareness, malware detection…the list goes on. In response, we have advanced our cyber capabilities and attracted world class talent.

Today, Herjavec Group is a global leader in cybersecurity with expertise in comprehensive security services including **Managed Security Services** (SOC Operations, Threat Detection, Security Technology Engineering) & **Professional Services** (Advisory Services, Identity Services, Technology Implementation, Threat Management & Incident Response). Herjavec Group is over 300 people strong, with offices and Security Operations Centers across the United States, United Kingdom, Canada and India. At Herjavec Group, we realize that in cybersecurity change is constant, but we are driven by a steadfast goal: to make enterprises around the world more secure.

To your success,

Robert Herjavec
Black Unicorn Awards Judge
Star of ABC's Shark Tank
Founder & CEO of Herjavec Group

Recognized Industry-Wide

MOST INNOVATIVE IAM PROVIDER
Cyber Defense Magazine Global Awards 2018 WINNER

SECURITY SERVICES LEADER
IDC Analyze the Future

LEADER IN MANAGED SECURITY SERVICES
Cyber Defense Magazine Global Awards 2018 WINNER

SECURITY COMPANY OF THE YEAR
CDM Cyber Defense Magazine

#1 ON THE
Cyber Security 500 — World's Hottest Security Companies

TOP 10 ON THE
2018 TOP 100 MSSPs — MSSPAlert.com/Top100

NIGHTDRAGON

"NightDragon *Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

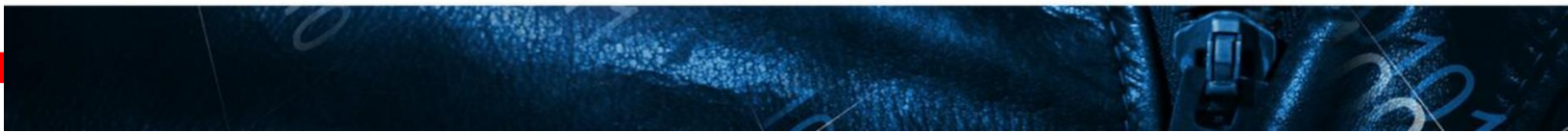
ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

available this spring...

From Bestselling Author Gary S. Miliefsky, fmDHS, CISSP



Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

***"At** Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. "*

Sean Drake
Managing Partner
Stony Lonesome Group LLC
203-247-2479
www.stonylonesomegroupllc.com

CYBER DEFENSE MAGAZINE RSA CONFERENCE 2020
SPECIAL EDITION SPONSORED BY:

AMERICAN HEALTH DEFENDERS

WWW.PANDEMICDEFENSEKIT.COM

INGERSOLL LOCKWOOD