CYBER DEFENSE MAGAZINE

2021 SPECIAL EDITION

Welcome to CDM's RSAC 2021 Issue

Once again, it's both an honor and a pleasure for our team to welcome readers to this Special RSA Conference Issue of Cyber Defense Magazine. Let me take this occasion to express thanks to Gary Miliefsky, our Publisher, and to Pierluigi Paganini, CDM International Editor-in-Chief.

Several unique qualities stand out in planning for participation in the 2021 RSA Conference. We would like to emphasize **creativity** in response to difficult circumstances, adoption of a **virtual** platform, and **steadfastness** in building on 30 years of solid history.

All of these qualities are reflected in the theme of **resilience** chosen to highlight this year's conference.

Whether the dynamic falls under theories like Darwinism, entropy, or the maxim that "Necessity is the mother of invention," every successful response to the challenge posed over the past year by the COVID-19 pandemic has included an element of *Resilience*.

We congratulate RSA for conducting this first virtual conference format. It will probably not be the last one to be held this way.

Let it serve as a testimonial for the powers of RSA to meet and exceed unusual demands, and in an environmentally sound manner.

The impressive list of speakers and article authors shows how RSA participants can overcome adversity, lead by example, and make ongoing contributions to cyber health and practice in a broad range of critical activities.

One of the successful ways CDM has brought attention to the leaders in cybersecurity is the Infosec Awards program: https://cyberdefenseawards.com/

Cyber Defense Media Group is pleased to have been an integral part of these trends with RSA for the past 9 years, and we look forward to sharing a bright future.

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 2021 Special Edition

It's hard to believe that it's been over a year since we all gathered for RSA Conference 2020 in San Francisco. So much has changed in our world since then. This past year has tested everyone's resolve in unique and unexpected ways, making the theme of RSA Conference 2021 -- *Resilience* -- resonate more than ever.

Here we are again, just weeks away from RSA Conference 2021, taking place virtually from May 17-20. While under ordinary circumstances, we'd be preparing to greet over 45,000 cybersecurity professionals, media, analysts and vendors to the Moscone Center, we could not be more excited to reveal an incredible digital-first experience that will combine the world-class content our audience has grown to expect with exciting new elements made possible by the virtual environment.

This year is also special for RSA Conference as it marks our 30th anniversary. In celebration of all that we have accomplished together throughout the past three decades, we have prepared one of our best programming lineups to-date. We look forward to bringing together the industry's greatest minds for more than more than 200 traditional and interactive sessions across 24 tracks for high-caliber and entertaining presentations and discussions. Our virtual keynote stage will be packed with thought-provoking content from industry visionaries, both RSAC veterans and newcomers alike, including a must-see fireside chat with the president and CEO of SolarWinds that will explore the technical elements of the breach and provide a deeper understanding into the most sophisticated supply chain attack in history.

But it doesn't stop there. Once again, attendees will have the chance to witness the next generation of cybersecurity innovators at the RSAC Innovation Sandbox. The impact of the competition has always extended far beyond the Conference stage and this year, while in a new digital format, will be no different. We also know how important networking is to our attendees, and RSA Conference 2021 will be loaded with opportunities to interact and collaborate with peers, sponsors, and experts. Every single program has been carefully designed to break down the barriers of virtual connection.

Every year brings new challenges -- to you, to your employees, to your organization -- and perhaps no year in recent memory threw us for a loop quite like 2020. The best weapon against these challenges? *Resilience.*

RSA Conference 2021 is the best place for the cybersecurity industry to come together to strengthen our resilience. From the first day to the last, attendees can expect to experience unending passion to evolve, adapt and do everything possible to protect the people and organizations that rely on us as their advocates.

We look forward to virtually convening in May!

Linda Gray Martin, Vice President, RSA Conference

RSAConference2021

May 17 – 20 | Virtual Experience

RESILIENCE

BIG NAMES.
BIG INSIGHTS.
BIG REASONS TO ATTEND RSAC 2021.

Over two hundred expert-led sessions covering 24 tracks. Thought-provoking keynotes. Cutting-edge innovation. Valuable networking opportunities. In-depth, interactive activities. RSAC 2021 is where the world talks security, and you can be a part of this important conversation.

Join industry leaders and peers at RSAC 2021, a virtual experience, May 17-20. Learn about the latest trends that are most relevant to your needs, advance your career and help shape the future of the industry.

Register today for the most inspirational four days in cybersecurity at rsaconference.com/cyberdefense21.

#RSAC

FOLLOW US

CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

• Deploy. • Manage. • Tune up. • Audit. • Defend. • Report.

GET YOUR FREE eBook

Get https://cionsystems.com/

Regula Delivers Remote Identity Verification for Everyone

A modern world requires modern solutions. Fraudsters constantly improve their skills; do not let your services lag behind!

By Arif Mamedov, Ph.D., President of Regula Forensics, Inc.

Previously an opportunity, nowadays a necessity: digitalization is spreading on a daily basis. Together with all the benefits it brings, organizations have to think one step ahead and mitigate the risks it brings. A recent study by Javelin Strategy & Research showed that identity fraud was as high as $56 billion in 2020. Interestingly, almost 1/3 of victims said that their financial service vendors did not provide enough safety measures and that this led to their decision to close their account with that particular vendor.

Considering that the average time spent on digital media in 2020 rose as high as more than 16 hours daily according to *The Wall Street Journal*, there is no doubt that an ideal sign-up process in a modern world should be: opening a web-page or a mobile application, scan, ready. Regardless of whether it is a car sharing app, financial services or even governmental services, it should be as easy as that. However, the aforementioned services require strict security as well as compliance with regulations.

That is where Regula's ID and identity verification steps in and can play a vital role. Increased daily online transactions require constant biometric verification, identity verification, fraud prevention and fraud mitigation in order to blend efficiency and security together.

In a digital world, being one step ahead of competition means bringing seamless experience throughout the entire customer journey. For instance, in aviation, travel and hospitality, delivering contactless check-in with the help of biometric and identity verification solutions can be as easy as taking a selfie or scanning a document.

Regula can also make retail and e-commerce operational work more secure and frictionless for the ‘new normal’. Imagine remote age verification or detection of likely fraudulent all together with no operational disruption.

Banks and other financial service providers want to ease the onboarding process, but they must not forget about the safety measures and ensure that they have the relevant security steps in place.

One of those steps is to know the identity of the user, or KYC (Know Your Customer). Regula gives you all the instruments to build your own, tailored KYC flow. Regula Document Reader SDK and Face SDK provides financial service providers with instruments that allow quick and easy onboarding for legitimate customers. The steps are not available to the fraudster, since they will not pass a face match check that is standard for this kind of security measure.

The constant increase in the need for an online presence has increased the need for remote identity verification among online retailers and governmental service providers. At the same time, new regulations around remote identification are putting the onus on such service providers to minimize the risks. So, it makes sense to choose a reliable product. Regula has more than 25 years of forensics experience, currently manufacturing hardware devices used by the majority of the governmental borders, as well as developing proprietary software for remote identity verification.

That was one of the reasons Regula was chosen as a partner to provide voter authentication in recent elections in Uganda. Identity-related fraud is the type of irregularity that happens most often during elections. In order to prevent that, election commissions in different countries tend to rely on biometric

technology. Regula Document reader SDK was used to scan and capture the image of the MRZ and its software then performed the recognition, extraction and parsing of the MRZ.

In addition to that, remote authentication also spread to the education sector. Regula recently partnered with global online testing giant, Pearson VUE, to help with the growing demand for safe and secure remote onboarding and authentication. Due to various lockdown measures and social and physical distancing policies put into place across the globe, there has been a dramatic rise in the need for remotely administered professional exams in a number of fields, including nursing, law enforcement and legal professionals.

This growth in online traffic has led to a proportionate growth in the need for secure remote onboarding and authentication solutions. To accomplish this, Pearson VUE turned to Regula and its advanced digital forensic technology to help secure its remote digital onboarding process.

Standing apart today for a lot of organizations means being transparent, secure, trustworthy and easy to use. To meet those standards and industry regulations Regula's in-house team develops fully on-premises solutions with an ID template database that is the largest on the market, containing more than 10,000 document templates from more than 248 countries and territories and covering 98 different languages. Both Regula's Document Reader and Face SDKs ensure maximum security for its customers.

About the Author

Arif Mamedov, Ph.D., President of Regula Forensics, Inc. Having rich experience in both hardware and software products Dr. Mamedov is a globally recognized expert in the field. He joined Regula back in 2010, and became an integral part of the company's growth .

Webpage: mobile.regulaforensics.com

endace

Critical Intelligence for the Cyber Front Line

Winning the cyber war depends on having visibility across the entire battlefield.

With Endace you can reduce investigations from hours to minutes with definitive evidence integrated into all your security tools.

endace.com

GTB Technologies
Data Security that Works™

West Palm Beach, FL USA

www.gtb.ai

+01 800.626.0557

GTB Technologies

Data Security that Works™

Data Security for the Cloud Generation

GTB Data Security that Works™ solutions protect data wherever it may be, with technology that was built to natively protect sensitive information and / or trade secret data with unsurpassed accuracy and ease of use

Compliance, All Channels

GTB detection technology has the rare capability of real time inspection & protection of secure content over all protocols.

Unsurpassed Accuracy

The unique proven ability to detect partial file matches on greater than 10 terabytes of unstructured file-less fingerprinted data

Time to Value

Highlighted as a Gartner Visionary by providing a comprehensive Enterprise Data Loss Prevention solution delivering a fast time to value

Solutions that Work

"GTB has the ability to control, protect, and secure my PII & PCI data, all in one place! GTB DLP is the superior alternative. "

100% Catch Rate!

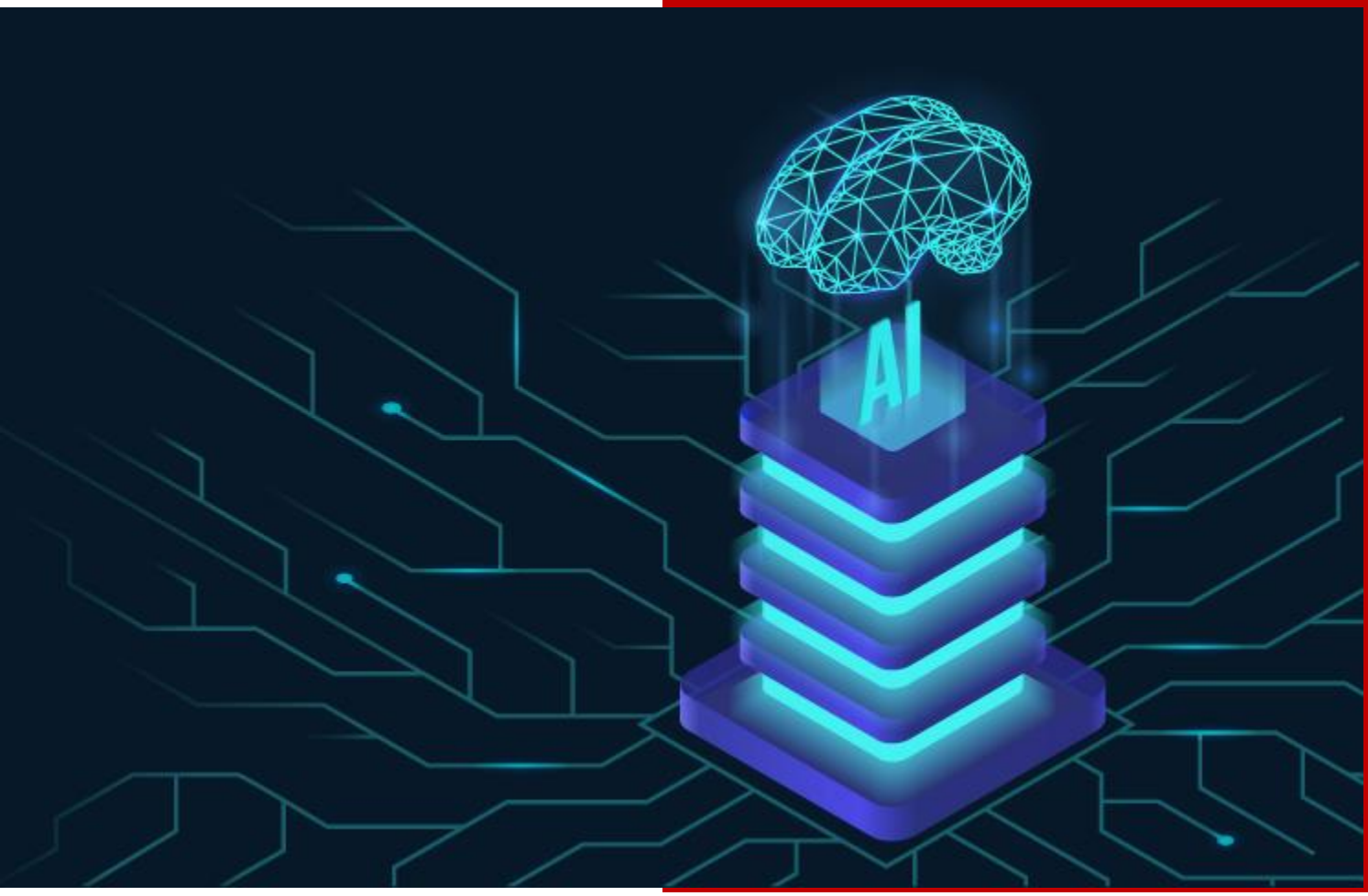
" What we liked: This product provides real granularity and reliability in catching data leakage. When using fingerprinted data, the catch rate is 100 percent, and no comparison data is saved.

What we didn't like: Nothing. This is a first rate product with some real innovations."

https://www.scmagazine.com/gtb-inspector-v12/review/5730/

Maximizing the Impact of AI/ML Threat Detection Tools

By Cary Wright, VP Product Management, Endace



Companies are increasingly looking to Artificial Intelligence (AI) and Machine Learning (ML) threat detection tools to improve the security posture of the enterprise. AI/ML shows great promise to detect previously invisible advanced persistent threats, insider activity, and new and emerging threats. These tools promise to detect threats that traditional network security tools miss by taking a radically different

approach to analyzing network activity. This alternate method of uncovering security threats may prove to be a pivotal technology in the struggle to protect critical infrastructure, important assets and sensitive data.

However, AI/ML threat detection tools require a significant investment in time and resources to deploy correctly to each environment. It's not enough to just throw them into an infrastructure: we need to make sure that we can trust the technology, and that it's attuned to our environment. It's imperative to make sure that it is deployed in such a way that increases efficiency, provides greater clarity into lurking threats, and reduces the number of alerts we investigate every day, rather than simply adding additional noise and workload to already overstretched security teams.

The promise of AI and ML

Adopting AI/ML threat detection tools is not about replacing existing security tools. Rather, it's about supplementing them with AI/ML to deliver additional capability and benefits.

AI/ML threat detection tools have the potential to significantly improve detection by identifying threats that other tools can't, especially at the earliest stages of the attack lifecycle. They can potentially detect emerging unknown threats such as Zero-day vulnerabilities - for which there are no existing 'signatures' - or threats that signature-based tools struggle to detect - such as fileless malware. And they can help associate related events to identify coordinated attack activity that might indicate a high priority threat while reducing the amount of "noise" caused by lots of individual event alerts. Their ability to detect abnormal behavior also enables them to spot potentially malicious "insider threats" other tools may miss.

The other potential benefit that AI/ML tools offer is to improve productivity by automating elements of the threat remediation process - particularly for commonly occurring threats - and thereby free up time for analysts to focus on the high-priority and more advanced threats.

Ultimately, AI/ML tools have the potential to automate many of the manual activities involved in SecOps, such as isolating suspected compromised hosts from the network and blocking access to the network from potentially compromised devices or users. The challenge is, however, that in order for security teams to hand over responsibility for these sorts of activities to an AI/ML tool, they need to be able to trust that tool to make the right decisions and know how it arrived at its decision. Otherwise, the danger is that

legitimate activity may be blocked and disrupt business activity, or alternatively malicious activity may be mistakenly identified as being OK and an alert not generated, leaving the organization open to risk.

Hurdles AI/ML detection tools must overcome

Despite their potential, AI/ML detection tools are not a panacea. They can miss threats and they can flag activities as malicious when they're not. In order for these tools to be trusted, the alerts they raise and the decisions they make need to be continually validated for accuracy.

If we train our AI and machine learning algorithms the wrong way, they risk creating even more noise, and alerting on things that are not real threats ("false positives"). This wastes analysts' time as they chase these phantoms unnecessarily, only to discover they're not real threats. Alternatively, they may also miss threats completely that should have been alerted on ("false negatives").

How do we guard against the pitfalls?

In the case of false positives, we need to validate that a detected event is not malicious and train the tool to ignore these situations in future - while at the same time ensuring this doesn't cause the tool not to alert on similar issues that are in fact malicious. The key to doing this effectively is having access to evidence that enables accurate and timely investigation of detected threats. Recorded packet history is an indispensable resource in this process - allowing analysts to determine precisely what happened and to accurately validate whether an identified threat is real or not.

Dealing with false negatives is more difficult. How can we determine whether a threat was missed that should have been detected? There are two main approaches to this. The first is to implement regular, proactive threat hunting to identify whether there are real threats that your detection tools - including AI/ML tools - are not detecting. Ultimately, threat hunting is a good habit to get into anyway, and if something is found that your AI/ML tool missed the first time around, it provides an opportunity to train it to correctly identify similar threats the next time.

The second approach is using simulation testing - of which one example is penetration testing. By creating simulated threats, companies can clearly see if their AI/ML threat detection tools are identifying them correctly or not. If they're not, it's once again an opportunity to train the tool to identify similar activity as a threat in future.

What's the architecture for a successful deployment?

For security teams, the ideal is to have a "single-pane-of-glass" that collects and collates threat telemetry from all of the different sources and provides a single view of threat activity across the threat lifecycle. Typically, organizations are electing to implement a SIEM tool, or a data-lake that provides data mining and search capabilities. SOAR tools are also rapidly gaining in popularity - as a way to help organizations collect and analyze evidence of threat activity.

The key capability that organizations need is being able to quickly reconstruct events from the collected and collated telemetry to understand what happened, how it happened, and what the impact of that event is. With a centralized view of activity, analysts can ask and answer questions quickly to understand whether there has been lateral movement from an initial compromise, whether data has been exfiltrated or not, etc.

Having access to full packet capture data is an indispensable resource in enabling this capability. With access to the actual packets, including payload, analysts can see what activity took place on the network and reconstruct events precisely - right down to seeing what data may have been exfiltrated and how an attacker is moving around the network to increase their foothold.

Full packet capture data is also an incredibly powerful resource for proactive threat hunting. Packet data-driven threat hunting and simulation exercises are a great way for teams to determine the effectiveness of their detection tools - including AI/ML tools - to understand why they are not detecting events that they ought to, or alternatively why they are incorrectly flagging non-malicious activity as malicious.

Packet capture data is invaluable as an evidence source because it is complete and reliable. Where a skilled attacker will often delete or modify logs to hide their activity, it's very difficult for them to manipulate packet data captured off the network - particularly when in most cases they are not even aware that it's being captured and don't have access to it. This makes packet data a trusted source of "truth" about what's really happening on the network.

Right deployment, right outcome

AI/ML detection tools have a lot of promise. However, there are pitfalls if the right architecture and capabilities are not in place. In order for AI/ML threat detection tools to deliver on their promise to reliably detect and remediate threats, companies must be able to trust them to make the right decisions, not to miss things, and to act accurately. To achieve this level of trust, we must be able to always verify and validate decisions made by AI/ML tools. To do this, companies need to ensure they have the right data.

Packets are an indispensable resource for validating AI decisions. But in order for packet data to be useful it needs to be complete and accurate, with no blind spots, and provide as much lookback history as possible. It also needs to be easily accessible and provide fast search and data mining.

Considering how packet data can be incorporated into workflows is also important. When packet data can be integrated into security tools - enabling analysts to pivot from a specific alert or event to the related

packets quickly and easily - the time it takes to investigate and resolve issues can be drastically reduced, dramatically increasing analyst productivity.

The right architectural approach is not one where AI/ML threat detection tools replace existing tools like IDS, firewalls and endpoint protection tools: it's one where they supplement them.

Alerts from your monitoring tools and other relevant evidence sources such as network flow data, log file data should all feed into a SIM/SIEM/Data Lake and SOAR tools so that analysts can operate from a "single-pane-of-glass" rather than having to bounce from tool to tool to see things. Packet evidence should be easily accessible from SIM/SIEM/Data Lake, SOAR tools and security tools such as IDS/IPS and firewalls to provide quick access for analysts and enable packet data to be accessed by automated processes such as SOAR playbooks.

With this architecture in place, companies can realize the promise of AI/ML technology to identify and remediate previously unknown threats at the earliest possible stage, with less noise and greater efficiency. Providing teams with integrated access to full network packet data is critical to ensure the accuracy and efficiency of AI/ML security tools and to ensure tools are properly tuned to match the environment in which it is deployed.

About the Author

Since 2017, **Cary Wright** has been Vice President of Product Management at Endace. With more than 25 years' experience in the telecommunications and networking industries at companies like Ixia and Agilent Technologies, he has been pivotal in creating market-defining products. Cary has an innate understanding of customers' needs and is instrumental in continuing the evolution of network recording and playback solutions and driving the growth of the Endace Fusion Partner program. www.endace.com

How Cobwebs Technologies' Webint Platform Helps Enterprises To Face The Rising Tide Of Security Risks Emerging From The Dark Web

The ai-based dark web monitoring capability provides a visual representation of cyber events, revealing a larger, graphically displayed picture as inter-connected dots of information based on collected data

By Udi Levy, Co-Founder and CEO, Cobwebs Technologies

Cobwebs Technologies announced today that several enterprises have deployed its AI-powered WEBINT platform for dark web monitoring to gain insight into emerging threats, or clues to breaches or attacks already in progress, aimed at them.

Sites and content on the dark web reside on overlay networks (darknet) that require specialized web browsers for access. The dark web is known as a place where stolen information from data breaches is sold and bought, paid for with cryptocurrency. Functioning as a black market, all kinds of illicit and stolen goods and services are for sale, including malware, ransomware, hacker toolkits, financial info, and personally identifiable information (PII) related to fraud. For threat actors, who know how to get on the dark web, the dark web is a way to interact online while remaining anonymous.

Stolen personal and corporate information, data breach leaks, and ransomware demands are major concerns for enterprises. The fallout can result in fines under privacy and data protection regulations, interruption of business operations, and brand damage. On dark web forums, threat actors can discuss topics that relate to ransomware, including breaches, cryptocurrencies, and extortion, while remaining anonymous.

"*In contrast to threat actors, it is very difficult for analysts and investigators to access the dark web, since it requires a special browser. Even if they would know how to access the dark web, exploring it to e.g., investigate criminal activities, requires a dark web search engine. Furthermore, by accessing the dark web themselves, analysts and investigators could be vulnerable to the scrutiny of threat actors related to the investigation. Our WEBINT solution is able to detect, collect, and analyze OSINT data from the surface, deep, and dark web, including threats, aimed at or related to an enterprise*," stated Shay Attias, Co-Founder & CTO of Cobwebs Technologies. "*With our solution, an enterprise can monitor the dark web-based on specific search terms or phrases without the need for its staff to access the dark web using a dark web browser to visit dark web websites, forums, and social networks. The AI-based dark web monitoring technology connects the dots in a visual graph and gives actionable insights in the form of automated reports that can be used for follow up by the enterprise itself and for law enforcement to take action*."

In general, dark web monitoring tools help investigators and analysts to identify threat actors, follow the cryptocurrency money trail, map connections between threat actors, their affiliates, and group members to solve and prevent crimes such as cyber threats. Dark web monitoring tools are also useful for detecting and preventing insider threats. Such dark web monitoring software can scan for direct mentions of a specific organization or specific assets that could indicate either being targeted or a potential breach. The dark web monitoring services also allow investigators to launch a cybercrime investigation with any small piece of digital forensics information, such as a threat actor's name, location, IP address, or image.

www.cobwebs.com

info@cobwebs.com

About the Author

Udi Levy is the CEO and Cofounder of Cobwebs Technologies. He brings vast experience in the global technology market with specialty in the Intelligence and Security domains.

Prior to founding Cobwebs, Mr. Levy and was responsible for developing Tactical & Cyber Intelligence Solutions in major companies and was involved in various strategic projects with Enterprises and Government entities.

Mr. Levy holds a BSc degree in Computers Engineering from the Hebrew University of Jerusalem and an MBA degree.

Udi can be reached online at (info@cobwebs.com, https://www.linkedin.com/company/10366794/) and at our company website http://www.cobwebs.com/

Read & verify identity documents on a Regula basis

98
languages

246
countries and territories

10k+
document templates

Onboarding Automation

Fraud Prevention

Automation of Check-in

KYC

Get in contact with Regula experts at **www.mobile.regulaforensics.com**

COBWEBS TECHNOLOGIES

AI-Powered Web Intelligence

Cobwebs Technologies is a world leading developer and provider of web intelligence solutions, powered by advanced artificial intelligence. Our innovative data-driven products are tailored to law enforcement and national security needs, identifying analyzing and monitoring threats in just one click.

Key Differentiators

- Discover Target Information
- Easy to Use
- Extract Locations
- Reveal Connections
- Gain Situational Awareness
- Real-Time Alerts

Watch Our Videos

Product Portfolio

Designed for investigators and tailored for their operational requirements, providing an enhanced yet user-friendly solution.

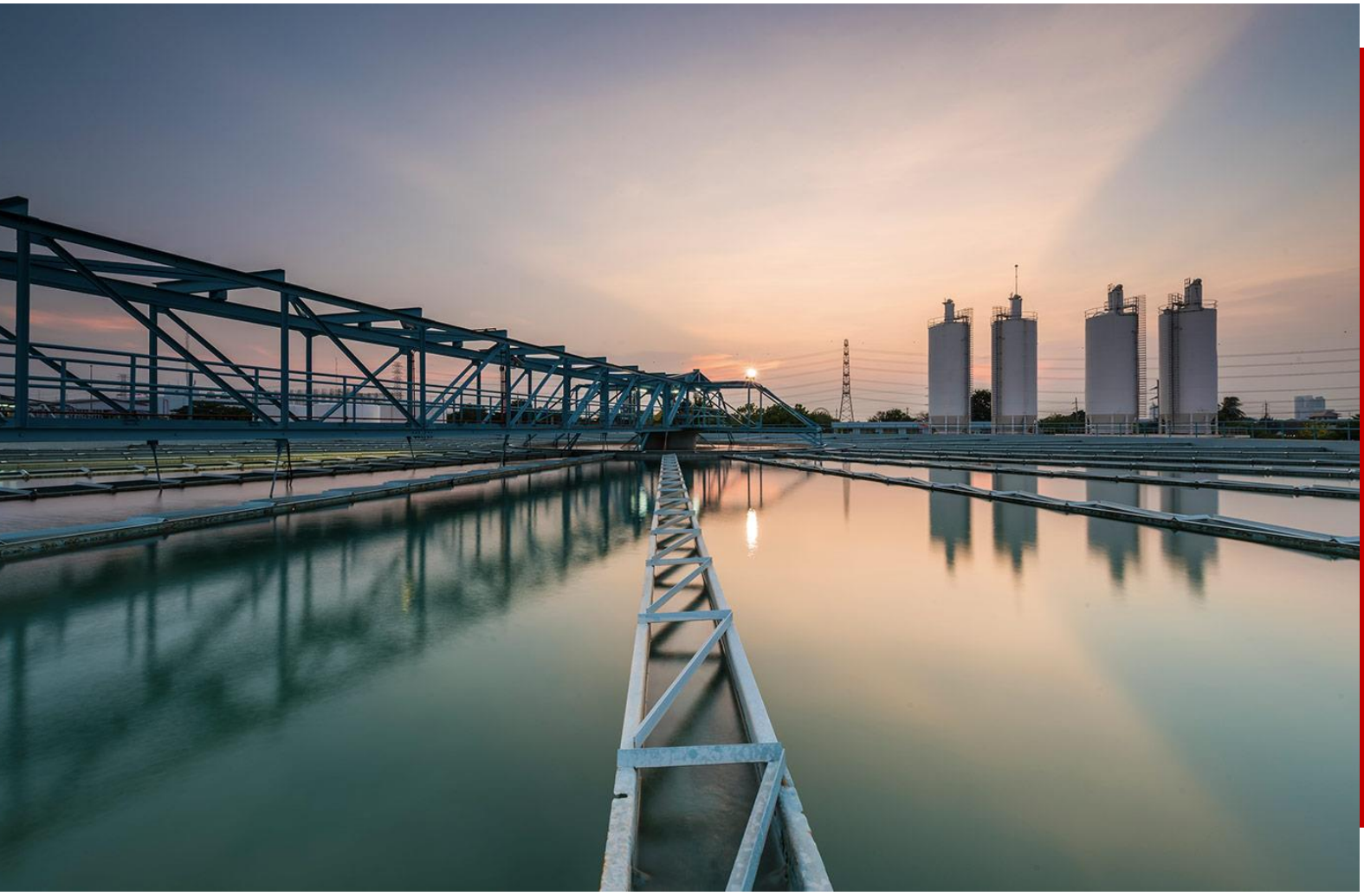
- Investigation Platform ›
- Location Intelligence ›
- Active Web Intelligence ›
- Financial Investigation ›
- Secured Analyst ›
- Threat Intelligence ›

Key Features

- Monitoring and analysis of social media, open, deep and dark web
- Transform a single lead into a developed, end-to-end investigation
- Identify target profiles and groups
- Extract geolocated data
- Live web data analysis and automated real-time alerts
- Streamlined artificial intelligence to provide automated insights

View Our Case Studies

+1 212 201 9256 | info@cobwebs.com
www.cobwebs.com



Takeaways from The Oldsmar Water Attack & What Security Leaders Can Do About It

With Real Examples & Screenshots of Cyber Attacks on Water & Wastewater Facilities

By Michael Yehoshua, VP of Global Marketing, SCADAfence

Over the last few months, cybersecurity journalists and the ICS security community have been discussing the Oldsmar Florida water system cyber-attack and other similar attacks on water infrastructure, almost ad nauseam. While many people have been talking about this "news" topic, we've actually been treating this issue with many of our customers over the past few years. In this article, I will explain what we've learned from this cyberattack, but most importantly, I will share how we've been busy solving these issues over the last few years with actual examples from our range of industrial cybersecurity products.

The Oldsmar Water Facility Attack

Back in February 5th, a hacker gained access into the water treatment system of Oldsmar, Florida, and hijacked the plant's operational controls. He was able to temporarily drive up the sodium hydroxide content in the water to poisonous levels. The Oldsmar facility is the primary source of drinking water for the city's 15,000 residents. Luckily, a plant operator was able to return the water to normal levels. The incident has nonetheless launched many conversations about the state of security in global critical infrastructure.

But that wasn't the whole story.

A security advisory released in March by the state of Massachusetts's Department of Environmental Protection, referred to additional unsafe practices or behaviors at the Oldsmar water treatment plant that significantly increased the risk further. Like many other facilities of its kind, Oldsmar uses a SCADA (Supervisory Control And Data Acquisition) system that allows staff to monitor and control conditions within the facility. At the same time, the staff was using TeamViewer, a fairly common remote access program, which can be used to monitor and control systems within the SCADA network. Sadly, cybersecurity was not a priority for the facility, as is the case occasionally with critical infrastructure. Not only was the Oldsmar facility using Windows 7 - an outdated software that is no longer supported by Microsoft, but all of their employees shared the same password to access TeamViewer. Additionally, the facility was connected directly to the internet without any type of firewall protection installed.

The Current Situation with Water Systems

In the United States alone, there are about 54,000 distinct drinking water systems. The vast majority of those systems serve less than 50,000 residents. They mainly rely on some type of remote access to monitor and/or administer their facilities. Many of their facilities are also unattended, underfunded, and do not have someone watching the IT operations 24/7. Finally, many facilities have not separated their OT (operational technology) networks from their safety systems that are in place in order to detect intrusions or potentially dangerous changes by threat actors.

While the attempt was spotted and taken care of by a plant operator before it could do any damage, it raises questions about how serious a threat this sort of terrorist or nation-state action could be in the future.

Why Don't We See More Stories Like This On The News?

So, despite how easy it is to find ways to remotely interact with such OT networks, we aren't seeing more incidents like the one in Oldsmar making the news. One reason may be that these facilities don't have to disclose such events right when they happen. Additionally, many companies, especially in the public sector want to avoid bad publicity and do what they can to avoid their company name smeared in cyber-attack news headlines. We've seen many companies, especially publicly traded companies lose stock value and brand trust after a cyberattack.

But the main reason you don't see more of these attacks on the news is that SCADAfence protects many of these critical infrastructure facilities.

Over the last seven years, SCADAfence has been working with many critical infrastructure organizations, including water & wastewater facilities to keep their OT networks safe. We do this by providing them with full network visibility, we accurately detect any anomalous behavior and malicious activities - including anomalies that originate in remote access. We were ready for 2020 before remote access security was required (due to the lockdowns) and it's been paying off dividends. Here is a case study of the City of Hutchinson, Kansas.

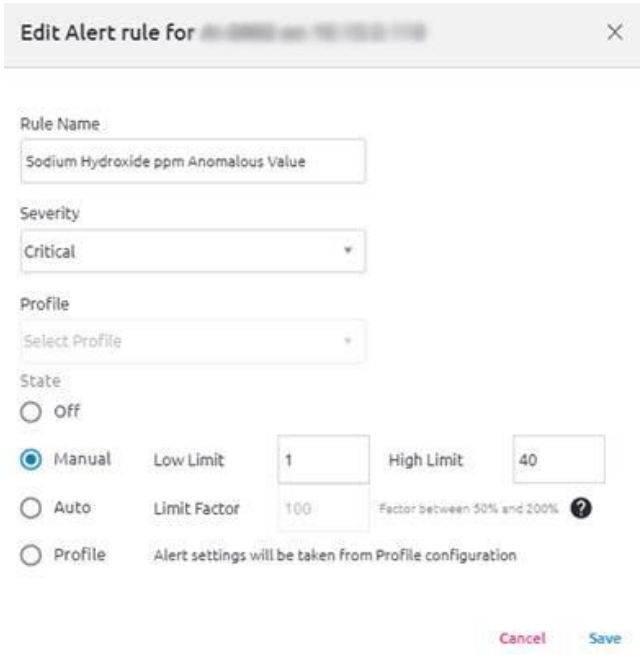
Here's How SCADAfence Secures Water Treatment Facilities

Let me show you a few key examples, (with actual screenshots) of how we have prevented identical attacks over the last seven years for our customers.

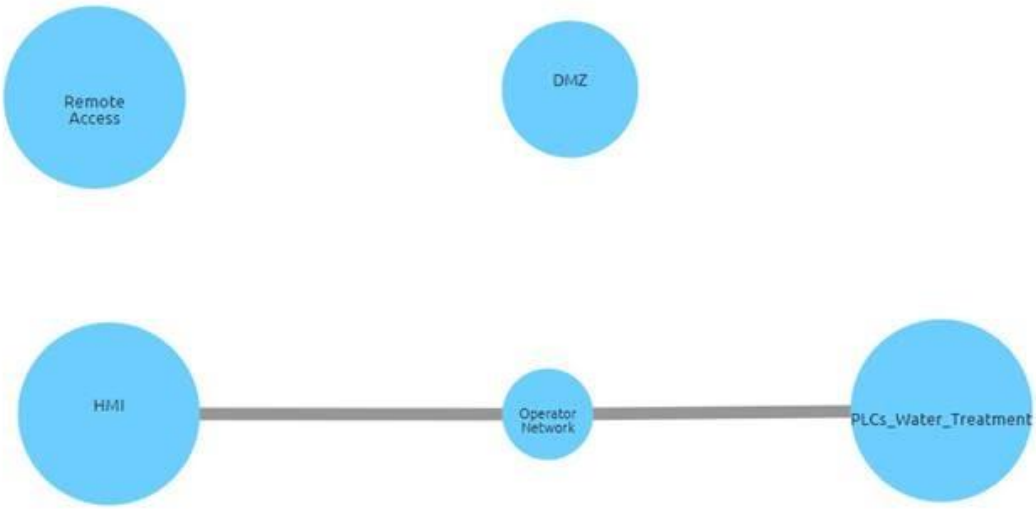
1. With the SCADAfence Platform's continuous network monitoring we have been easily been able to detect any remote access into OT networks, specifically, detailed alerts for TeamViewer connections in OT networks.

2. We also immediately alert on value level changes, once they pass a certain threshold to prevent unauthorized changes or process manipulation. The platform is also so flexible that users can create specific firewall-like rules for variables such as this one: "Sodium Hydroxide ppm

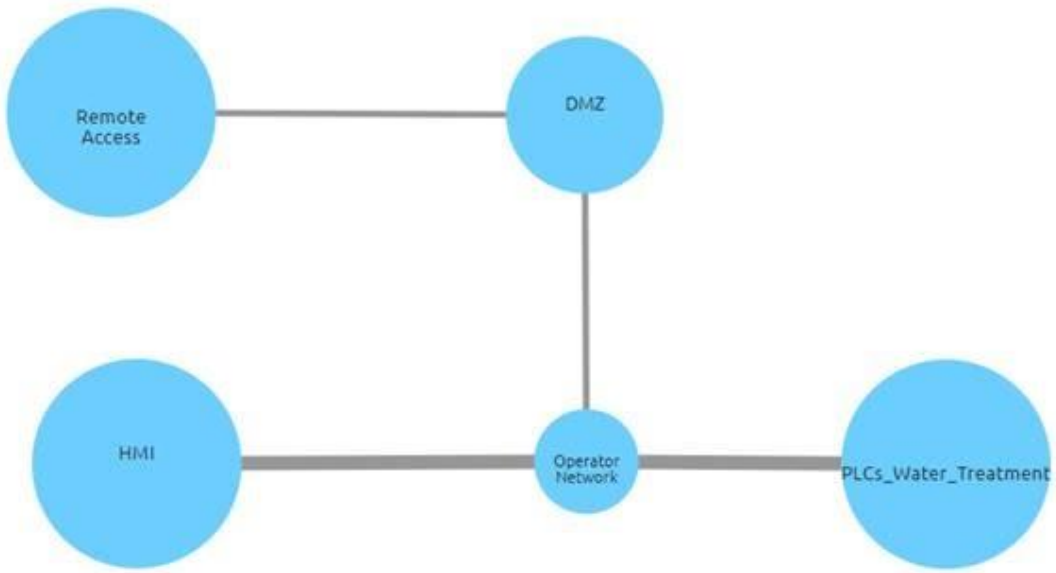
Anomalous Value" alert. This will raise an alert in case the value of Sodium Hydroxide in the water exceeds the max value of (for example) 40 ppm (parts per million) or goes below 1 ppm.



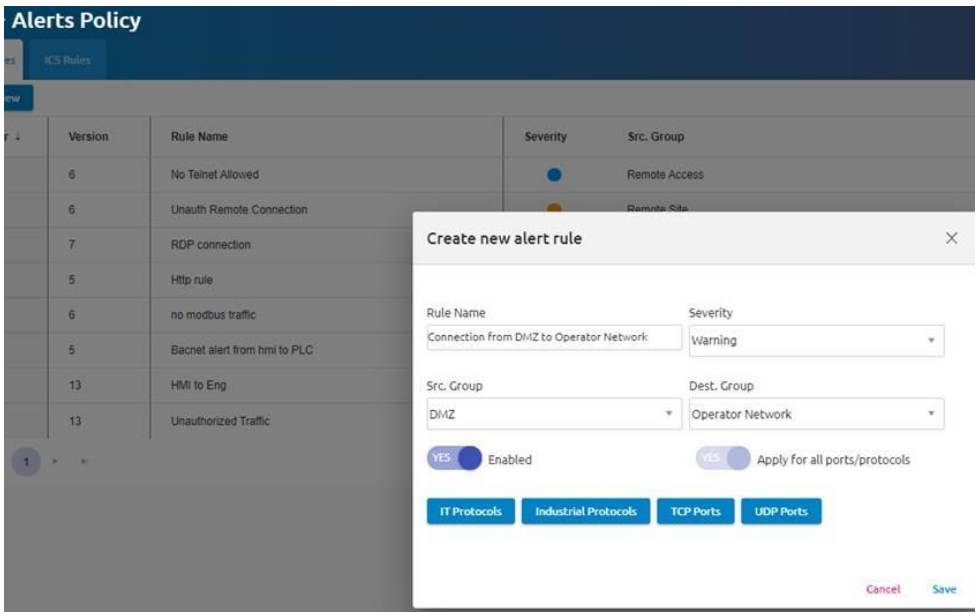
3. The SCADAfence Platform also provides visual exposure maps that can spot malicious activities - weeks, or even months in advance. At another similar incident (that didn't hit the news), we monitored a water treatment facility during normal operations. As you can see in the screenshot below, there was no connectivity between the remote access group and the DMZ group.

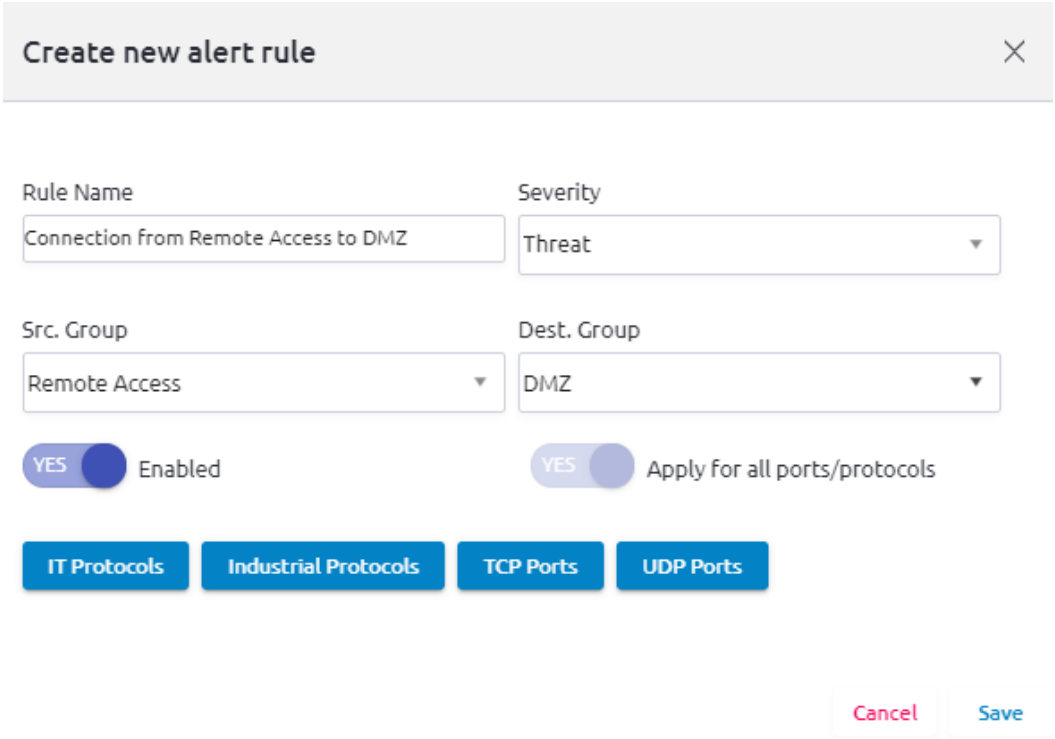


During an attack on the facility, the security team was immediately able to see new connections forming from the remote access group to the DMZ group and from the DMZ to the operator network group (see below). As soon as that alert was issued, the security team was notified of that change and the remote access connection was disconnected, stopping the attackers immediately.



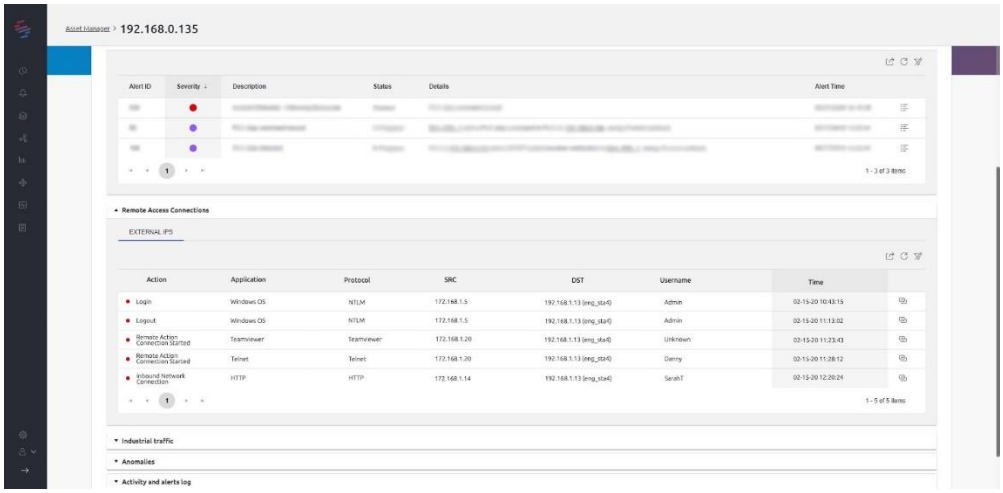
4. It's really easy to set automated rules that will alert in case there is connectivity between specific network groups. In this case, we set an alert if there is a connection from the DMZ to the operator network and a similar rule in case there is a connection from the remote access to the DMZ group.



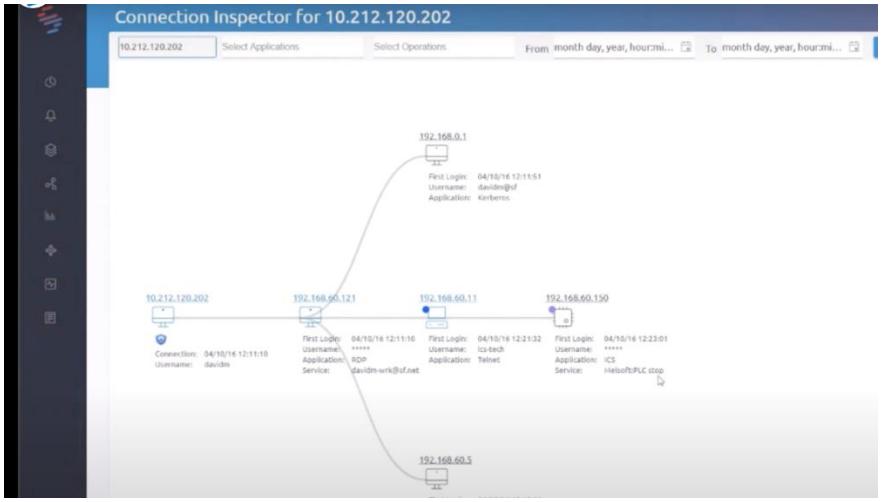


5. This incident at Oldsmar, highlights what we've been saying for years. Remote access in OT networks provides a big risk. And the thing is, remote access is not going away.

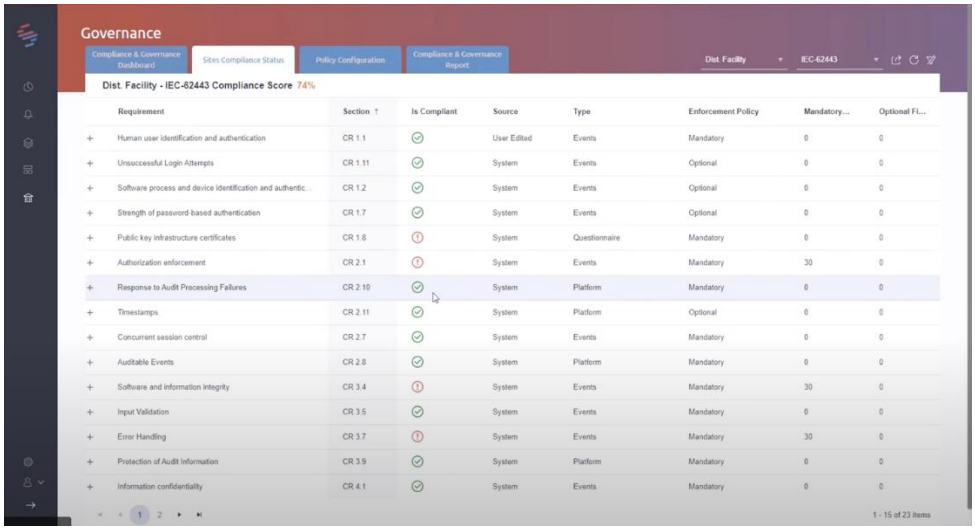
The SCADAfence platform also provides security staff with the correlation between their users and their activities while performing remote work.



In addition to alerts on anomalous or unauthorized actions in the OT network, the SCADAfence Platform provides security teams with the association details - including the user name, the originating workstation, and the application to provide a holistic view into remote access activities, hop-to-hop.



6. This also ties into the issue of compliance with industrial standards. SCADAfence offers a governance portal that enables operators to define compliance enforcement policies, and continuously monitor compliance enforcement status for most ICS standards, frameworks, and regulations.



Don't Be Scared, Be Prepared

Many water & wastewater utilities are already using continuous network monitoring and remote access technologies to get visibility into their OT networks and keep their critical infrastructure networks secure.

With this holistic approach, of network monitoring, anomaly detection, remote access visibility, and compliance, many water & wastewater are already reducing 95% of their risk level of future attacks.

The best part is that these solutions are all agentless, are not intrusive, and can perform superhuman tasks at a fraction of the cost of one human worker.

If your organization is looking into securing their industrial networks, the experts at SCADAfence are seasoned veterans in this space and can show you how it's done.

To learn more about these products and see short product demos, click here: https://l.scadafence.com/demo

About the Author

Michael brings 15 years of marketing creativity and out-of-the-box thinking to SCADAfence. Before joining the team, Michael was the Director of Marketing at TrapX Security, where he was famous for thought leadership and for turning a small, declining startup into a successful, profitable world-leading vendor in their vertical. Prior to that, Michael was the VP of Marketing at AMC and rebuilt their entire marketing architecture, bringing in strong revenue figures that the firm has't seen in decades. Michael studied at Harvard Business School, at Bar Ilan University for his MBA & Lander College for his BS degrees in Marketing and Business Management.

Michael can be reached online at (marketing@scadafence.com, https://www.linkedin.com/in/michael-yehoshua/) and at our company website https://www.scadafence.com/

Concierge Cybersecurity & Privacy™ Platform

BLACKCLOAK™

Are cybercriminals targeting your company through your executives?

Executives' personal lives are often the weakest link to accessing your critical corporate data. With **BlackCloak**, you'll be covered.

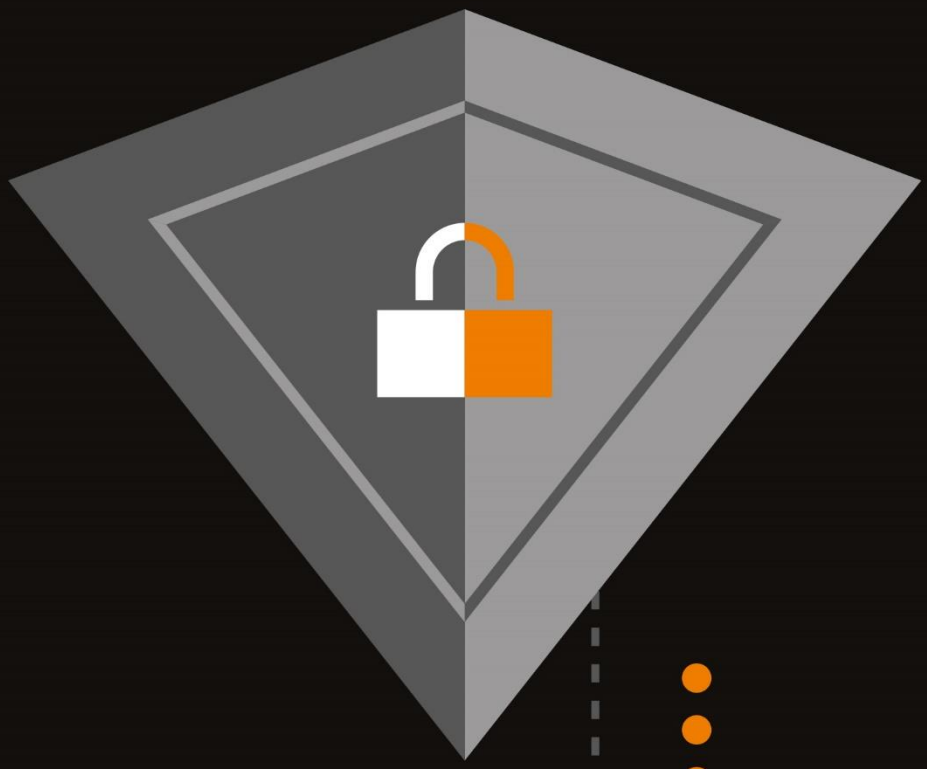
Protect Your Executives. Protect Your Company.

Get BlackCloak / blackcloak.io

Build a safer digital society

We are Europe's leading go-to security services provider, supporting your business globally.

orangecyberdefense.com



Orange
Cyberdefense

orange™

Trust Not in Third-Parties

You aren't on your own in cybersecurity, but you should act like you are

By Gregory Hoffer, CEO, Coviant Software

Cybersecurity management is a dynamic process. There is no "set it and forget it." Things move fast, conditions change constantly, and often the things that change happen beyond your control or notice. For organizations heavily invested in cloud services, the applications and computing instances you rely may change moment-to-moment. It's hard to keep up.

Modern IT infrastructure is a mélange of on premises and cloud, hardware and software, owned and subscribed, in-house and third-party, fixed and ephemeral. And even if you have a handle on monitoring your IT estate, you've still got to pay attention to conditions affecting your direct and indirect partner relationships. The recent SolarWinds breach was a reminder of the ways criminal hackers can exploit weaknesses in the digital supply chain to work their way into target networks. But there is another threat that can take advantage of vulnerabilities in third-party systems and relationships that does not get the attention it deserves.

The high-tech industry changes quickly. Innovators come on the scene with new ways to solve old problems and, with the backing of venture capital, aggressively work to build market share. Mid-market players merge to create momentum. Large companies buy startups to add capabilities without incurring undue risk. Stockholders, founders, and venture capitalists, all eager to make money on their investments, push for deals that will turn them a profit, disrupting markets and often creating chaos for customers.

Wall Street tracks these mergers and acquisitions. When a public company is involved in the deal, it can affect stock prices and so it's important for portfolio managers to pay attention. Industry analysts track these moves in an effort to provide guidance to clients who want to know what it means for them. Hackers pay attention to these developments, too. M&A activity often affects the security posture of organizations that are users of the technology or applications involved.

After a company has been acquired, major changes to the product typically follow. That can mean products that are redundant to the acquirer's catalog are killed and the customers migrated to the incumbent, or customer service and support teams that had developed detailed institutional knowledge of their users are not retained and the responsibilities shifted to new personnel or even outsourced. That can result in vulnerabilities that go undiscovered, unpatched, and exploitable.

When disruption affects products that organizations rely on to keep data safe, the implications can be serious. The managed file transfer (MFT) industry, where Coviant Software operates, is one such example. MFT products are a foundational element in data management and security programs, and their essential role is reflected in an annual growth rate of over 10%, and market value that will exceed $3 billion by 2026, according to Global Market Insights. That value has attracted M&A activity resulting in industry consolidation, with a number of key players getting purchased by larger organizations.

In one case, a twenty-year-old file transfer appliance in wide use got caught between the obsolescence of its operating system and the release of its newly designed replacement. Hackers took advantage of the lapse and breached a number of well-known companies, including the Kroger supermarket chain and Royal Dutch Shell, operator of Shell gas stations. According to *TechRepublic*, the appliance was left vulnerable to exploitation by a common SQL injection attack, and while it is hard for an outsider to know the details of any data breach, experts familiar with the situation suggest that resources and attention were shifted from the legacy product to the replacement. Meanwhile, the operating system's maker ended its support of the product, and so patches were not being written and distributed.

Poor communication and coordination seem to be the common thread in the breaches that resulted, prompting one security expert to recommend to *TechRepublic* that organizations "do a closer analysis of

any legacy/near-end-of-life products which may no longer be receiving the expected vulnerability testing efforts."

Sometimes M&A activity can have security implications on a scale well beyond the product level. Consider the scenario hospitality giant Marriott International faced after acquiring the Starwood Hotel chain. What Marriott didn't know was that Starwood's IT systems had been compromised by hackers before the acquisition took place. In this case the hackers laid low, choosing to passively monitor their victim for many months and so the breach went undetected. After the two organizations were integrated, however, the hackers began siphoning off data, resulting one of the largest breaches of consumer data to date.

While customers might expect to be informed of major changes to the products and services they use, it doesn't always happen, and so the responsibility is ultimately on the enterprise to take ownership of their own security, even if that means assuming that any component, software, or application that it does not have complete control over is likely already compromised. From there, the organization must exercise diligent, continuous testing of all systems in order to ensure changes in status are detected, security gaps are identified, and proper action is taken to close those gaps quickly.

It can be easy to think that, because a vendor or service provider markets their offerings on security, you don't have to worry about it. But as the lessons of cybertheory tell us, organizations can't rely on others to address their data security needs. Trust not in third-parties. Do your due diligence when making purchasing decisions, and keep the conversation going. Pay attention to changes and, if one of your partners or vendors is involved in any market deals—directly or indirectly—find out what the implications are for your organization.

Vendors and service providers should regard their customers and subscriber relationships as more than merely transactional. But just because you've invested your trust in them doesn't mean they will continue to earn that trust. No organization is perfect; adversaries are counting on it.

About the Author

Gregory Hoffer is CEO of Coviant Software, maker of the secure, managed file transfer platform Diplomat MFT. Greg's career spans two decades of successful organizational leadership and award-winning product development. He was instrumental in establishing ground-breaking technology partnerships that helped accomplish Federal Information Processing Standards (FIPS), the DMZ Gateway, OpenPGP, and other features essential for protecting large files and data in transit.

For more information visit Coviant Software online, or follow Coviant Software on Twitter.

A New Era of Malware Analysis

By Stas Gaivoronskii, a Malware Analyst at ANY.RUN

Malware is a constant threat to organizations around the world. Open an email and you may lose a lot of money, data, and reputation. Different tools can help to overcome these situations.

After the attack cybersecurity analytics usually collect and investigate a malicious program to find out its type and functions. The best way to do this safely is by sandboxing.

There are several tools that researchers use for investigating malware. However, malicious programs get smarter, and they can identify a virtual machine. Botnets, Trojans, RATs, and others focus on small details that can ruin the whole analysis: they require user interaction, specific software versions, etc.

To install different operating systems and set additional programs whenever malware doesn't show up – can be time-consuming and expensive. Thankfully, there is a unique solution that both saves your money and speeds up analysis. ANY.RUN service can do it all.

A new trend for detecting and investigation

ANY.RUN is a cloud-based interactive sandbox. Analysts use it to detect malware and investigate incidents. Moreover, a large sample database of IOCs and ready-made reports can improve the everyday work of a cybersecurity specialist.

The service has an interactive approach to the analysis of malicious content that other sandboxes are lacking. The malware analysis takes place in real-time, and you are directly involved in the process.

In a matter of seconds, you get a ready-made workplace where you can run malicious files. There is no need to configure additional tools for logging file events and network traffic. This is what ANY.RUN offers, and unlike many systems, it doesn't limit you in the number of submissions.

Nowadays, it is not enough to run a suspicious file in an automated detection system to conclude that it's secure. Some types of threats (such as APTs) require direct human interaction during analysis. Our toolset for online malware analysis allows you to monitor the research process and make adjustments when necessary, just as you would do when working with a real system. There is no need to rely only on automated detection.

A new interactive approach in real-time

Let's have a look at what stands for interactive access in ANY.RUN. During your investigation in real-time you can:

- Move and click a mouse, input data, reboot the system, open files – any kind of interaction with the virtual environment is possible;
- Change the settings: pre-installed soft set, several OSs with different bit-versions, and builds are ready for you;
- Download files and modules;
- Research network connections;
- Monitor systems processes;
- Collect incident indicators;
- Get Mitre attack matrix;
- Have a process graph.

All of these features help to reveal sophisticated malware and see the anatomy of the attack in real-time.

A new way to get results faster and easier

The interactivity of ANY.RUN allows you to get initial results immediately after starting the task. The whole process often takes just a few seconds.

The service is easy for cybersecurity professionals and junior specialists. ANY.RUN makes malware analysis as simple and straightforward as possible for users of any level. Thanks to the user-friendly interface, anybody can start working with the service right away, without lots of instructions.

The cloud service allows you to run an analysis on any device anywhere in the world without using your computer's resources. There's no need to buy additional servers, software, or hardware.

The new era of malware analysis has begun – fast results, tamed advanced malware, not a complicated process of research, and detailed reports. If you want to be a part of it, just join ANY.RUN community. Request a demo version, and get interactive analysis for free!

About the Author

Stas Gaivoronskii is a malware analyst at ANY.RUN, the first interactive online malware analysis sandbox. He has more than 9 years of experience in the digital forensics field and 2 years in malware analysis.

Stas can be reached out online at s.gaivoronsky@any.run and at our company website https://any.run/.

ANITIAN

Get your cloud apps to market fast and start unlocking revenue in just weeks – *not* months or years.

Anitian's automated, pre-engineered Compliance Automation Platform and Secure**Cloud** Service make new or existing cloud applications secure, compliant, and market-ready up to 80% faster and at half the cost.

www.anitian.com

RECOVER + PROTECT

Industry-leading data security solutions

Driving Innovation
Since 2007

SECURE DATA™

Visit
SecureData.com

Legacy ERP Applications and Data Security: Closing the Gaps

By Piyush Pandey, CEO, Appsian Security

ERP applications have historically had a reputation for being complex systems with equal parts value and challenge. Value in that they can be uniquely tailored to an organization's business processes. But challenging because the complexity of those business processes typically leaves organizations exposed to a myriad of data security risks. ERP applications house the most sensitive PII, financial, accounting, and proprietary data an organization may have. That puts ERP data in the unique position of being routinely accessed by many users within the organization (in an authorized manner) while being highly coveted by bad actors.

In short, ERP data is the "crown jewels" of an organization.

The sensitive nature of these crown jewels makes them an attractive target for a variety of security threats like phishing attacks, payroll diversion, zero-day, brute force attacks, and exploit by malicious insiders. To thwart these advanced threats, businesses invest in NGFW, IDS/IPS, VPN, and SIEM solutions. Unfortunately, most of these solutions monitor and control north-south traffic but have no visibility into what is happening within the applications – leaving significant visibility gaps. Plus, access governance is dictated by broad-bucketed, static roles that leave many opportunities for risk, as the context of user access (different locations, devices, connection points, etc.) changes with various contextual scenarios. These variations are the origins of risk.

This means that control and visibility gaps are widening as business processes become more complex, and user access to ERP applications becomes more ubiquitous. These gaps are only exacerbated by legacy ERP applications like PeopleSoft, Oracle EBS, and SAP ECC that were not designed to combat modern threats. In fact, they were designed to replace manual, paper processes and were designed to provide as much access to data and transactions as possible – in service to enabling productivity.

For many organizations, legacy ERP applications have been deployed on-premise and continuously customized for decades. The customizable nature is a highly desirable characteristic, but that also means there are not many widely adopted best practices for protecting the security at the application/user interface layer. Each organization handles data security differently, and the sophistication of the strategies can vary widely. Throw in the 2020 shift to remote workforces, and present-day ERP data security strategies are far from adequate for protecting the crown jewels.

Moreover, the ERP security threat landscape is dynamic, consisting of application vulnerabilities and bad actors compromising data. To keep up with security maintenance, organizations must update applications and operating systems and apply security patches – creating an extremely cumbersome process. These initiatives require cross-functional collaboration across IT, information security, and HRIS teams, and any configuration errors can lead to ERP downtime, costing thousands of dollars every hour. Cyber-criminals can leverage these pitfalls and typically can impersonate an authorized user to stay undetected and exfiltrate sensitive data. And sadly, organizations can take over two months to contain an insider threat, as indicated in the latest Ponemon reports.

In 2021, amongst a sea of security threats, organizations must adopt proactive, dynamic ERP data security strategies to overcome the shortcomings of reactive security controls. This is precisely why Appsian Security works with hundreds of legacy ERP customers who have been using applications like PeopleSoft, Oracle EBS, and SAP for decades.

The Appsian Security Platform (ASP) combines sophisticated controls to strengthen authentication, dynamically control user access, limit the exposure of sensitive data, and provide granular visibility into ERP data access and usage. ASP installs directly into the ERP web server without adding customizations, hardware, or complexity and provides:

- **Granular Visibility and Real-Time Analytics:** Sophisticated logging captures granular user activity, while data access and usage data are aggregated and visualized on actionable dashboards – designed to quickly uncover potential threats and enable a rapid response.
- **Fine-Grained, Dynamic Access Controls and Data Security:** Native integration of enterprise IAM solutions like SSO and MFA for dynamic user authentication. Enhance existing static controls with dynamic, attribute-based access controls that enable best practices like least privilege and zero trust. Lastly, expand the use of dynamic, policy-based data masking across all desired data fields with one-to-many implementation.
- **Automate and Accelerate Audit and Compliance:** Analyze deviations in user behavior and uncover potentially damaging data policy violations. Leverage pre-built compliance reports for SOX, GDPR, CCPA, among others, to help ease the audit response for complex regulatory requirements.

The Appsian Security Platform is a sophisticated web application firewall with multiple features working simultaneously to provide a comprehensive solution for filling the data security gaps of legacy ERP applications. All, without adding complexity to your IT and information security organizations.

Key customer benefits include helping legacy ERP customers:

- **Secure Access Beyond the Firewall**
  Use dynamic, risk-aware controls to allow or restrict access to data based on context.
- **Mitigate Business Process Risks**
  Deploy fine-grained controls inside sensitive business transactions that reduce your financial risk exposure.
- **Modernize Legacy ERP Security & Compliance**
  Legacy ERP applications that cannot combat advanced threats.
- **Rapid Threat Detection & Response**
  Have a real-time, granular view into data access & usage. Be proactively alerted to anomalies that can lead to data breaches, fraud, theft, and error.

Appsian Security was formed over a decade ago by core team members of the PeopleSoft corporate strategy group. The management team has accumulated ERP experience of 100+ years. If you have ERP systems, we can secure them!

To learn more, visit http://www.appsian.com/.

About the Author

My Name is Piyush Pandey. I am the CEO of Appsian Security. I am a technology executive with two decades of global experience in strategy, sales, mergers & acquisitions, and operations within software companies. Over the last ten years, I have worked with enterprise software companies including Oracle, Epicor, Concur, Citrix, and Microsoft on various transactions. I have held various leadership positions at Procera, Deutsche Bank, Stifel, Wipro Technologies, and a wireless startup.

Piyush can be reached at piyush.pandey@appsian.com and the company website http://www.appsian.com/

Identity Crisis? It's Time to Take the Holistic Approach

By Jerome Becquart, COO, Axiad

In planning for a secure future hybrid working reality, many IT leaders have reconsidered how they manage the identities on their network. Their workforce now uses new systems and devices, interacts with the helpdesk entirely remotely, and needs to access their resources from dispersed locations. Businesses are investing in new technology to protect their remote workers, but are still faced with rising security threats – 90% of IT leaders reported an increase in cyberattacks since the pandemic.

Here at Axiad, we speak with customers every day about to adapt their business processes to this new reality, without sacrificing security – whether they're wondering how to prevent escalating phishing threats, automate their credential management process, or encourage employees to follow best security practices. Many of them feel overwhelmed by the number of new technologies they need to address all of these concerns.

Cybersecurity can be hard enough without an identity crisis. That's why we're sharing our tips on how to take the holistic approach to consider all the identities on your network and fully secure them all.

Tip 1: Think about every identity within your organization

The first mistake a lot of organizations make when planning their identity management strategy is not considering every identity on their network. Sure, a lot think about their users and what types of credentials they'll need for their various systems. But what about the numerous machines on a company's network, like mobile devices, servers, applications, and IoT devices? Machines are dramatically increasing, and require a solution that will identify these identities, authenticate them, and then secure their interactions across the network.

IT leaders need to consider PKI-based solutions for managing their machine identities, so their IT teams can issue certificates to their machines, track what is on their network, and encrypt the communication between the devices. This will prevent falsified entities from entering the network and putting data at risk. With the scalable Axiad PKI solution, businesses can continually issue and manage digital certificates for every type of machine as they join the network.

Tip 2: Consider how to verify emails and documents crossing your network

In the face of phishing threats, many companies focus their investments in anti-malware software or new technology to prevent the threats from getting through. Unfortunately, some of these emails will inevitably slip through the cracks. That's why we recommend IT leaders take an identity-centric approach to help their employees secure their emails and protect themselves against scams.

Enterprises should implement email and document signing with certificates to accomplish this. By digitally signing emails, email recipients can quickly confirm the identity of the sender and ensure that the email is legitimate. The same goes for documents – if you can digitally sign a contract or purchase request with a certificate, your business can operate with a higher level of trust. This also reduces the wet-ink hassle of printing and scanning documents while working remotely.

Tip 3: Enable simplified identity credential management for IT and end users

Amid the transition to the hybrid workforce, both your IT team and your employees are likely stretched thin. As you deploy new credentials to protect access to your enterprise resources, your IT team is likely focusing on managing the systems instead of doing strategic work. And with each new credential, your end users are spending more time issuing and managing each tool. Often, they end up reaching out to the help desk for assistance, stretching IT resources even thinner.

Credential management should be automated for your IT team, and simple for your employees to manage. Your business can do this by offering them a unified experience for all your various credentials. Our Axiad Cloud solution offers one place where both IT teams and employees can issue, manage, and troubleshoot their various credentials whether they're hardware tokens, smartcards, TPM, mobile authenticators, etc. End users no longer need to juggle different software and don't need to ask IT for help, allowing everyone to focus on moving your business forward.

Tip 4: Know, trust, and verify every user before issuing credentials

When considering every identity, you need to manage and secure, many enterprises struggle to first verify the identity of their employees, end customers, or partners before issuing them their credential. With the increase of digital interactions, your business needs to find a streamlined solution to reduce identity fraud, follow regulations, and ultimately ensure complete trust for every entity. Many traditional identity verifications processes are slow and filled with red tape, meaning that identity verification can't keep pace with the rest of a digitally transformed business.

That's why identity proofing technology is essential for businesses that need to ensure customers or users are who they say they are. Adopting an identity proofing solution accelerates verification with ID document and biometric capture. This reduces the delays of regular verification, which means customer acquisition and employee or partner onboarding can be completed easily and efficiently.

Tip 5: Maintain a high standard for identity assurance

Your business can invest in multiple identity credentials to defend every use case and identity on your network, but it all goes to waste if users don't follow best practices or find workarounds in your system. If you're faced with a dispersed workforce, it can be even harder to ensure all your employees are adhering to your security policies and are using their required authentication tools.

Airlock, a key feature of Axiad Cloud, allows your IT team to assign employees specific directives before they can gain full access to the company system. This means that if they need to activate a new authentication device, update a certificate, or unlock their device, Airlock will require them to take that action before they can work on any other projects. Businesses can have peace of mind that no matter where your employees are, they are consistently meeting the standards your business needs to operate securely.

Final thoughts

In the age of digital transformation, it's time to take a holistic approach. It isn't enough to authenticate just your users, businesses need to authenticate all their identities – whether its their systems, machines, etc. – and ensure trusted and secure interactions among them. You also need to consider the long-term impact of the IAM solutions you're selecting. Solutions that are automated and user-centric will simplify identity management for both your IT team and your employees, so you can ensure end-to-end security.

About the Author

Jerome Becquart is the COO of Axiad. He has over 20 years of experience in identity and access management solutions, including 15 years at ActivIdentity. Jerome's management experience includes roles in operational management, sales management, professional services, product and solution marketing, engineering, and technical support. After the acquisition of ActivIdentity by HID Global in 2010, Jerome served as general manager of the HID Identity Assurance business unit. He chaired the Global Platform Government Task Force for three years, and served on the board of directors of this Industry organization.

Jerome can be reached online at https://www.linkedin.com/in/jbecquart/ and at our company website https://www.axiad.com/

ANY RUN
INTERACTIVE MALWARE ANALYSIS

https://any.run

Analyze malware online in the sandbox

Malware Hunting

Use a unique interactive approach to work with the virtual environment.

Try the full power of interactive analysis for free.

Get fast results in a few minutes.

Manage your team and work on the same task together.

Investigate more than 2 million public submissions.

Enjoy a UX-friendly interface suitable for all kinds of cyber specialists.

axiad

Passwordless Anywhere with **SMARTidentity**

Secure digital interactions for users and machines to keep your business moving forward

axiad.com

Manage the Cloud Permissions Gap to Achieve Zero Trust

The Cloud Permissions Gap exposes organizations to highly exploitable risk combined with the inability to implement and manage Zero Trust policies.

By Raj Mallempati, CloudKnox Security COO

In 2020, when organizations were prioritizing digital transformation so they could pivot to remote work on an unprecedented scale, Gartner added a new category to its 2020 Hype Cycle for Identity and Access Management Technologies called Cloud Infrastructure Entitlement Management (CIEM).

CIEM? Looks a lot like SIEM.

CIEM may look like and even sound like SIEM (security information and event management), but the two security solutions are not the same. While there may be some overlapping capabilities for cloud-first and hybrid environments with cloud-native SIEM vendors, none of them have the ability to extend their platform to manage and enforce entitlements and permissions for the multi-cloud and hybrid cloud enterprises. This management and enforcement of entitlements and permissions is a core competency of a comprehensive CIEM platform, and it enables organizations to design and implement Zero Trust architectures in multi-cloud and hybrid cloud environments. As multi-cloud adoption continues to increase across the industry, the movement of workloads to such environments requires in-depth visibility and analysis of cloud infrastructure accounts, permissions, entitlements and activity, and granular controls.

Why is CIEM vital for organizations? The Cloud Permissions Gap.

A new attack surface has emerged in response to mass digital transformation: the Cloud Permissions Gap. CloudKnox threat research has uncovered that more than 90% of privileged identities within organizations' cloud infrastructures (both human and machine) are using less than 5% of their permissions granted. This delta is known as the Cloud Permissions Gap, and it is a contributing factor to the rise of both accidental and malicious insider threats impacting enterprises of all sizes, as attackers are able to exploit an identity with misconfigured permissions and access across the organization's critical cloud infrastructure.

Specific risks and challenges associated with the Cloud Permissions Gap include:

- **Inactive identities and super identities.** Every company has at least few inactive identities—former employees, testing, POCs, etc.—just hanging out there. Even more dire, there are other identities known as "break-glass accounts" or super identities that are floating around with unlimited permissions and unrestricted access to all cloud resources offered across the organization.
- **Over-permissioned active identities.** Continuously tracking and monitoring the proliferation of new services, roles and permissions in the cloud is almost impossible to do manually.
- **Cross-account access.** Organizations leverage cross-account roles to allow identities to access different environments—development, test, production, etc.—and allow third-party entities to access their accounts. This is both convenient and a potential vulnerability for the organization. The inherent danger is when an identity access management (IAM) role in these instances is over-provisioned. Since these roles grant permissions to an entire account, the misconfigured permissions tied to the role can cause significant—and costly—ripple effects.
- **Anomalous behavior among machine identities.** Machine or non-human identities consist of scrips, bots, access keys and others, and they typically perform the same repetitive actions. If a

machine identity executes an action it has never performed on a resource that it has never accessed, chances are someone is misusing the credentials.

The Cloud Permissions Gap exposes organizations to highly exploitable risk combined with the inability to implement and manage Zero Trust policies. This is why enterprises adopting cloud-first strategies must leverage a multi-cloud entitlements and permissions management platform that provides comprehensive visibility, automated remediation, continuous monitoring and compliance.

How to close the Cloud Permissions Gap with CIEM

CIEM is the next generation of solutions for managing access and enforcing least privilege and Zero Trust access in the cloud. With the benefit of a SaaS offering that deploys in minutes with full up-and-running capabilities in 24 hours or less, here are three ways CIEM can help organizations secure their cloud infrastructure right now:

1. **Leverage activity-based authorization to right-size permissions of identities.**

   To accomplish this, the organization empowered by a CIEM solution would remove or scope down permissions for over-privileged users, service accounts and groups automatically. Then it would enable high-risk permissions on demand with controlled timed access using an integrated approval workflow, restricting broad access to critical cloud infrastructure resources.

2. **Identify, improve and monitor Identity and Access Management (IAM) hygiene continuously.**

   A CIEM solution allows the organization to migrate from static, assumption-based permission grant processes to continuous, activity-based permissions management processes—helping the organization to monitor, get alerts and remediate anomalous identity behavior, unauthorized identities and roles.

3. **Implement automated, continuous compliance and reporting.**

   To remain compliant and secure, it is essential that organizations restrict access to virtual machines. CIEM can help by removing inbound Secure Shell (SSH) and remote desktop (RDP) access in security groups automatically. Organizations leveraging CIEM can also adopt best practices, such as enabling multi factor authentication (MFA) for all identities with console access; rotating credentials and manage keys regularly; and automating custom risk reports across all accounts using NIST 800-53, CIS Benchmarks and AWS Well-Architectured reporting to drive compliance.

The Cloud Permissions Gap across an organization's cloud infrastructure is exponentially getting more dangerous as bad actors exploit those identities to exfiltrate sensitive information from growing attack vectors. By instituting best practices for cloud permissions and entitlements management and leveraging automated technologies that reinforce those best practices—like CIEM—organizations will be better suited to protect critical cloud infrastructure resources and identities in their hybrid and multi-cloud environments. Organizations continuing to prioritize digital transformation and cloud-first strategies are not complete without a robust, scalable CIEM platform, especially as they strive to implement a Zero Trust architecture.

To learn more, please check out the following resources:

1) State of Cloud Entitlements Report

2) Achieve Least Privilege at Cloud Scale with a Cloud Infrastructure Entitlement Management (CIEM) Solution

3) Get a Free Cloud Infrastructure Risk Assessment

About the Author

Raj Mallempati recently joined CloudKnox Security as Chief Operating Officer, where he is responsible for CloudKnox's overall business and go-to-market strategies. Prior to joining CloudKnox, Raj was most recently the SVP of Marketing at Malwarebytes. Raj has also held positions as the VP of Global Marketing at MobileIron, VP of Product Marketing at Riverbed Technology, and was the Director of Marketing and Business Strategy at VMware. He holds an MBA from The Wharton School, University of Pennsylvania, MS, Computer Science from the University of Texas, and a B.Tech from Indian Institute of Technology, Madras.

5 Cybersecurity Predictions for 2021

By Rajesh Khazanchi, CEO at ColorTokens

Transformation happens fast in today's world of information security. Sometimes history is an indicator of how things will change, and sometimes a once-in-a-generation pandemic comes along and shows us a future we could never have predicted. With 2020 behind us, the threats it spawned have opened a new cybersecurity landscape. So, what might we predict that 2021 will bring?

#1. No Speed Limit on Cloud Migration

There's no doubt that in 2020, while companies scrambled with lockdowns taking place worldwide, many realized that they don't have business resilience built into their IT operations. As companies quickly came to terms with their on-premise deployments lacking resilience, the already rapidly increasing cloud adoption rate was compounded and will continue into 2021.

Companies that didn't have a significant digital channel were also greatly impacted as they struggled to adapt in 2020. For this reason, many companies will be focused on the rapid growth of their digital channel, which will further drive the acceleration of moving to the cloud in 2021.

#2. Zero Trust to Hit Mainstream

The traditional castle-and-moat approach of creating a security perimeter has repeatedly shown to be ineffective against sophisticated attacks. Its assumption that users, endpoints, applications, workloads, and traffic within a network can be inherently trusted is flawed. This incorrect assumption allows for any threats within the network to move laterally and remain undetected. And, with remote work being the new norm, the attack surface for cyberthreats has expanded exponentially.

This has paved the way for the mainstream embrace of Zero Trust architecture in 2021. With a Zero Trust approach, every user, application, workload, and network flow is assumed untrusted. This micro-level approach ensures that access requests are monitored and verified at every point within a network, shrinking the attack surface to a bare minimum.

Cloud-delivered solutions like the ColorTokens Xtended ZeroTrust™ Platform are making Zero Trust a reality for any enterprise, including SMBs, which will not be spared in the years ahead. As enterprises seek to stay ahead of evolving cyberthreats, such Zero Trust projects and their mainstream embrace will take off in 2021.

#3. Granular Access Appeals

As the new normal sets in, providing granular user access controls are taking center stage as a 2021 security initiative. The world has moved to work from everywhere, and workforces spread across the globe demand access to critical data and applications. A fine-grained, dynamic framework is needed to effectively control access of remote employees, contractors, suppliers, and vendors to resources and data.

Businesses that solely address the static factor of user trust, (i.e., passwords or biometrics), one of The 4 Trust Dimensions, will be a prime target for cyberattacks in the new year. In 2021, expect to see enterprises investing in solutions that address multiple trust dimensions of user access and enforce fine-grained policies based on context.

#4. Cloud Citizenship

A shift to cloud-native applications has been driven by innovation, scalability, and efficiency. The way today's applications are being built is significantly shifting into the microservices and container world. We can expect a big move from virtualized applications to cloud-native applications in 2021. As this wave of cloud citizenship rides into the new year, powerful, cloud-based policy engines, like what we've built at ColorTokens, will be needed to automatically extend security controls to new cloud-native applications to eliminate exposure and secure them from internal and external threats.

#5. Unification Uptake

Buying multiple point solutions has complicated security postures and IT operations, and most enterprises are recognizing they need to make a security shift. With a unified platform, businesses can break free from point solutions performing siloed functions, and can instead address their networks, applications, users, and devices using a single integrated solution and unified view. This growing pace of organizations turning to a single, unified security platform over traditional point solutions will continue into 2021 and beyond.

About the Author

Rajesh Khazanchi is a cybersecurity pioneer who's been on the front lines of the battle against cyberattacks for nearly three decades. As a security entrepreneur and executive, Rajesh is motivated by the ideal that no one - not businesses, not families, not individuals - should be forced to feel the pain of a cyberattack. That's what fuels his work at ColorTokens. Prior to ColorTokens, Rajesh led product development teams at HP, Oracle, and VMware. He has been awarded six patents for his innovations in cloud automation and cybersecurity. Rajesh can be reached online at @ColorTokensInc. and at our company website https://colortokens.com

COLORTOKENS

Trust in Zero Trust.

A **New Mindset** for New Challenges

Cloud adoption is growing
Traditional perimeters are re-defined
New attack vectors are materializing

Xtended ZeroTrust™ Platform

ColorTokens utilizes rich, meaningful and contextual information about the workload, application, micro-service or resource being protected to apply Zero Trust with as secure a perimeter as you can.

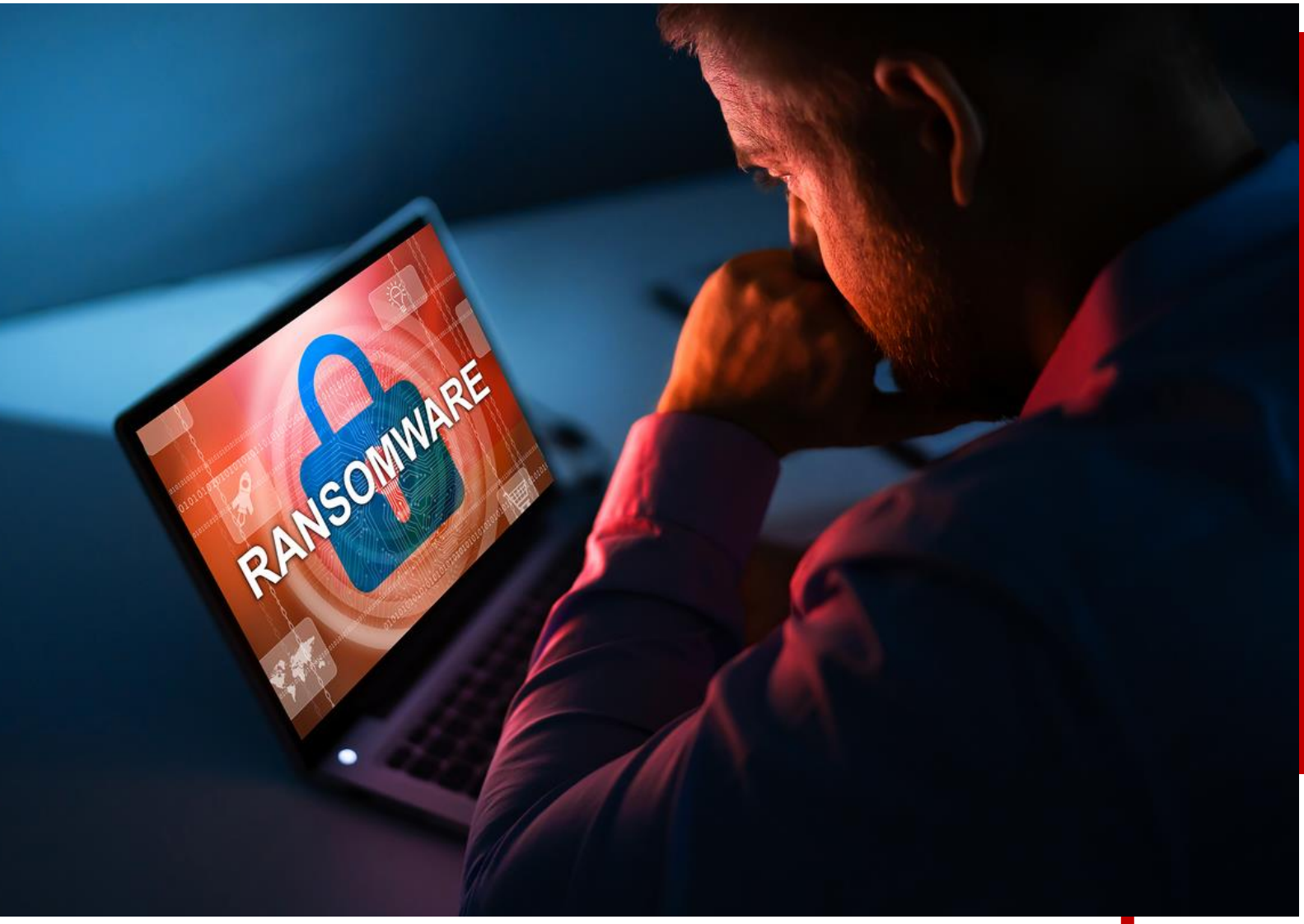
70%
Reduction in Compliance Costs

80%
Reduction in Security Alerts

100%
Faster Deployment

Contact Us

Santa Clara · New York · London · Copenhagen · Bengaluru



The Rise of Ransomware

Understanding the Surge in Cyber Extortion

By Jamie Wilson, Founder and Chairman, Cryptoloc

Ransomware is on the rise, and it's not slowing down. Cryptoloc founder and chairman Jamie Wilson explains the perfect storm of conditions that have combined to allow ransomware to run rampant – and how organizations can protect themselves.

For most of the world, the past 12 months have been defined by COVID-19. But for cybersecurity professionals, it's the rise of ransomware that has set off alarm bells. Of course, these two scourges are not mutually exclusive.

Now, there's nothing particularly new or novel about the concept of ransomware – the practice of locking a victim out of their own files and demanding a ransom for their decryption dates back to at least the mid-2000s. What is deeply concerning, however, is how frequent and impactful these cyberattacks have become.

Ransomware on the rise

Ransomware attacks dealt unprecedented damage to organizations in 2020. The FBI reported a 400 per cent increase in cyberattacks after the onset of COVID-19, while a report into the economic impact of cybercrime by McAfee and the Centre for Strategic and International Studies (CSIS) found that company losses due to cyberattacks had reached almost $1 trillion in the United States alone by late 2020.

Whereas a typical ransomware attack against an individual may once have netted the attacker a few hundred dollars, increasingly savvy cybercriminals now target organizations, extracting hundreds of thousands of dollars from each 'successful' attack and helping to drive small and medium-sized enterprises out of business.

One attack in 2020 against German IT company Software AG came with a staggering $20 million ransom demand. Another German attack took a terrible toll in September, when a woman in need of urgent medical care died after being re-routed to a hospital further away while Duesseldorf University Hospital dealt with a ransomware attack.

A report by defense think tank the Royal United Services Institute (RUSI) and cybersecurity company BAE Systems found that the number of groups launching ransomware attacks grew month on month throughout 2020, and that most of these groups are now utilizing a tactic known as 'double extortion' – not only do they force organizations to pay a ransom to operate their systems and unlock their encrypted files, but they also threaten to leak the data, intellectual property and other sensitive information in those files if the ransom isn't paid.

Cybercriminal group Maze is thought to have been the first to employ the double extortion tactic in late 2019, and it's since been used in attacks against major companies like Travelex, CWT and Garmin.

Consider the impact an attack like this could have on, for instance, a travel agency – not only could they be locked out of their own booking system, but they could face further consequences if the client details they have on file, including passports and driver's licenses, are leaked.

Further complicating matters is the uncertainty about how long a cybercriminal might have been in your system. It's one thing to back up your files every seven days, for instance, but if they've had access to your system for months, that's redundant – and makes recovery close to impossible.

The perfect storm

There are any number of factors that have led to the surge in ransomware over the past 12 months, from the increasing ease of its use to the changes in the workplace caused by COVID-19 and the frequency of ransom payments.

The aforementioned report by RUSI and BAE Systems points to how easy it has become for cybercriminals to acquire and Utilize ransomware, exemplified by the rise of ransomware-as-a-service. Even low-skilled cybercriminals can now pay a fee to nefarious operations like REvil for pre-packaged ransomware that they can use. Shady operators can even employ the services of 'initial access brokers', who sell access to pre-compromised corporate networks.

It's long been known that ransomware attacks exploit human weaknesses as well as technical vulnerabilities, and the boom in remote working caused by COVID-19 has presented cybercriminals with plenty of both. The FBI attributed the sharp spike in cyber-crime in 2020 to ill-secured virtual work environments and a reliance on email and makeshift IT infrastructures.

It's a free-for-all that led to a dramatic increase in risk, as businesses caught flat-footed by the pandemic lost track of which devices were being used by their employees, and had no control over the security of their Wi-Fi connections. With employees operating across different networks in multiple locations, using the same devices for work and personal purposes without the benefit of their organization's security perimeter, the attack surface for cybercriminals grew exponentially.

Once an attacker compromises an employee at home, it's just a matter of waiting for them to connect to the corporate network. From there, they may as well be plugged into a computer inside the office.

Often, organizations will feel they have no choice but to pay the ransom – and the more organizations that give in, the more that ransomware is normalized and incentivized. And while taking out a cyber insurance policy might seem like the responsible thing to do, it further encourages payment, turning ransomware into just another standard operating cost.

It should be noted, too, that the rise of ransomware is inextricably linked to the rise of cryptocurrencies like Bitcoin – a secure, essentially untraceable method of making and receiving payments favored by cybercriminals for its anonymity.

I've seen organizations faced with the difficult choice of whether or not to pay the ransom firsthand. While there is momentum behind a push to make ransom payment illegal, it's entirely understandable that

victims would feel they have no choice but to pay up – especially when sensitive personal data or medical records are at stake, or, as in the case of Duesseldorf University Hospital, a life hangs in the balance.

Consider, too, initiatives like the General Data Protection Regulation (GDPR), which places the possessors of personally identifiable information at greater risk of substantial fines if that data is leaked, and it's clear that ransomware is a legal and ethical minefield that can only be successfully navigated by steering well clear of it in the first place.

An end to ransomware

With ransomware posing an increasingly serious threat to all organizations, it's essential to take precautions – but not everybody is getting the message.

McAfee and CSIS surveyed nearly 1,000 organizations late last year and found that only 44 per cent had cyber preparedness and incident response plans in place. Worse yet, just 32 per cent of respondents believed their plan was actually effective.

The obvious first step, especially in light of the remote working boom, is to ensure timely patching of all your organization's software and devices. While this won't guarantee protection against attack, it will minimize your exposure.

Education is a key component of this. Organizations need to ensure that all of their employees are aware of the importance of timely patching, and regularly briefed on the latest techniques being utilized by cybercriminals. It's every organization's responsibility to engage their employees with that training – it may seem time-consuming, but it's vastly preferable to the alternative.

Above all else, though, is data. Organizations need to control who has access to their data, and know exactly what they do with it. My company, Cryptoloc, is dedicated to protecting that data – which is why we've developed the world's safest cybersecurity platform.

Our patented technology – developed in collaboration with an elite team of cryptographers, mathematicians, data scientists and software developers – combines three different encryption algorithms into one unique multilayer process. It can be deployed across a wide range of applications, including file storage, document management and delivery, and counterfeit prevention and detection solutions. Our clients can send fully encrypted documents straight from Microsoft Outlook, and develop and build their own products on our secure digital platform.

Our ISO-certified technologies ensure that organizations and their employees, contractors, clients and customers can interact securely, with each piece of data assigned its own separate audit trail, and every user and action verified and accounted for.

Better yet, our 'Zero Knowledge' protocols mean we know nothing about the data our clients store with us. Our escrow encryption key recovery process ensures their data is theirs and theirs alone, and can only be accessed by the people they choose.

No other platform has ever been able to guarantee the same protection as Cryptoloc – and in today's landscape, that's the level of protection required to prevent attackers from exploiting vulnerabilities and installing ransomware.

Ransomware will only stop when ransomware is no longer profitable, and that will only happen when organizations stop falling victim to ransomware attacks. They have to have absolute certainty that they control their data – and in doing so, they can control their future.

About the Author

Jamie Wilson is the founder and chairman of Cryptoloc, recognized by Forbes as one of the 20 Best Cybersecurity Startups to Watch in 2020. Headquartered in Brisbane, Australia, with offices in Japan, US, South Africa and the UK, Cryptoloc have developed the world's strongest encryption technology and the world's safest cybersecurity platform, ensuring clients have complete control over their data. Jamie can be reached online at www.linkedin.com/in/jamie-wilson-07424a68 and at www.cryptoloc.com

RSA Conference 2021

May 17 – 20 | Virtual Experience

RESILIENCE

FOUR DAYS OF CYBERSECURITY INSIGHTS, NOW AVAILABLE ON DEMAND.

RSA Conference 2021 was a virtual gathering spot for cybersecurity's best minds who shared their knowledge and experience with thousands of attendees over four days.

Here's your chance to catch up on all the insights you missed: Register today for an On Demand Pass for just $295. Dive into over 200 informative sessions and stirring keynotes covering timely topics such as ransomware, machine learning, IoT security and much more.

Don't miss this opportunity to hear new perspectives and learn about the latest threats and trends so you can expand your knowledge and help keep your organization secure.

Register today for your On Demand Pass at rsaconference.com/cyberdefense21.

#RSAC

FOLLOW US


HOW TO BECOME UNATTRACTIVE FOR CYBER-CRIMINALS
Sweepatic offers an easy-to-use 24x7 Attack Surface Management Platform to map, monitor and manage your online exposure. Use our platform to close all virtual doors and make your company unattractive to cybercriminals.
Request your free, personalized demo!
www.sweepatic.com/demo
sweepatic SECURITY

SecOps as a Service; The Future of Cybersecurity

By Manoj Arora, CEO & Founder, Difenda

The cybersecurity industry was a different place when I founded Difenda in 2008. I saw the same issue over and over again—companies misled by the cybersecurity “leaders.”

Technology resellers promising the impossible. Vendors overselling functionality. Managed services focusing on the wrong things. A disconnected cybersecurity processes. There was no uniformity in the industry and it led to poor customer experiences across the board.

I wanted to change that dynamic—to create a company that was all-in on the customer’s outcome. This trend motivated me to start Difenda. Through this journey, I made an important discovery. I saw that the future of cybersecurity needs to be an integrated, connected, and collaborative experience that unified departments and provided total visibility into the people, processes, and technology that drive companies forward. I knew this would be a sustainable strategy - and based on Difenda’s growth over the last 13 years, we must have done something right.

Reinventing Managed Services

Let me start by saying that I passionately believe success in cybersecurity is a by-product of customers' success. Customer outcomes should always be the top priority.

So, how did we – Difenda – go from an unknown start-up to one of Microsoft’s leading North American partners, and their go-to partner for complex Azure Sentinel deployments and MDR services? It comes down to the aforementioned success. Difenda started its first cybersecurity operations center in 2013. Since then, we have served a wide variety of customers in extremely data-sensitive industries like banking, finance, insurance, healthcare, and mining.

While most service providers offered managed services as an add-on to their product resale, we took a different approach. Focusing on customer success, we completely reengineered our managed service offering from the ground up, concentrating on integrity, sustainability, and the competence expected from a Security Operations Center (SOC).

Upon relocating our SOC to Oakville, Ontario, we doubled down on our customer success paradigm by building our ISO 27001 Cyber Command Center (C3) in 2016, using some of the most advanced security operations technology available. The following year, our continued success was recognized in 2017 when we were invited by Cyber New Brunswick's to establish a presence in Fredericton, New Brunswick, Canada, as part of a public-private partnership to fight cyber threats to critical infrastructure across the country. In dedication to this partnership, we established a secondary Cyber Command Center in Fredericton

Throughout our growth, we’ve retained our ISO 27001 Certification, SOC2 Type 2 Certification, and are one of very few highly certified Cyber Command Centers operating within North America. Difenda has been recognized by IDC Canada as a major cybersecurity service provider for the last five years in a row and has been featured in the Top 100 Canadian Companies several times in the past.

Why does our success story matter? The answer is simple - despite many companies making significant cybersecurity investments, there was still a substantial need for self-sustain cybersecurity operations. Focusing on the customer – we always want to set them up for success, and as I stated earlier – if they cybersecurity customer is winning, the service provider is winning.

Our success highlights this need; Enter the rise of SecOps-As-A-Service and the shift to integrated cybersecurity.

SecOps as a Service: Defining the Next Generation of Cybersecurity

Despite our success, companies were still getting breached and hacked despite the millions of dollars spent acquiring “cutting-edge” cybersecurity tools. This led to the rapid, unsustainable growth of conventional SecOps, forcing organizations to look at innovative ways to address their risk landscape.

It was clear, however, to us, that delivering a transformational, innovative approach to delivering sustainable cybersecurity operations was working. Here’s how we at Difenda approach this problem streamlined service offerings to cater to an outcome-based approach. This was a deliberate decision made to focus on building deep-rooted capabilities in threat life cycle management, which included:

• Threat Modelling

• Threat Detection

• Threat Response

And then the ‘Ah-ha’ moment in 2019. The critical moment still defines our strategy today. We partnered with Microsoft to beta test their latest solution—Azure Sentinel.

We knew our customers wanted to consolidate. They wanted better visibility into their cybersecurity processes. They needed to turn data into a competitive advantage to enable decision-making. They needed data to be accessible to justify decisions to internal leadership, boards, and other stakeholders.

What Microsoft was offering was the answer. It was the realized dream of a unified cybersecurity solution. It was the first real example of what SecOps as a service and integrated cybersecurity could be. It was the rise of the connected solution, one that leveraged all data available to allow companies to make the best decisions possible. It was a solution that best used the latest technological innovations.

We were sold.

We knew exactly what a unified Microsoft solution could do against modern threats. And since then, we’ve established deep expertise and capabilities in providing best-in-class MDR services using Microsoft’s comprehensive portfolio of security technologies. And the best thing for our Microsoft clients? A service provider that focused on it.

Difenda Shield: A New Approach to a New Paradigm

We took that experience with Microsoft to revamp our cybersecurity offerings, and continue to offer sustainable, long-term solutions. The results? We created a fully integrated catalog of services through our Difenda Shield platform. This modular approach to SecOps leverages all of the data collected through other Difenda Shield components to provide full visibility of an organization's people, processes, and technologies.

Here's what our integrated cybersecurity solution looks like today:

• **Difenda Shield Portal:** This is where all the mission-critical data is collected and processed to generate the powerful insights an organization needs to make the best security decisions. Every Difenda Shield component feed into this portal providing customers full visibility into their security operations live on demand.

• **Difenda Shield MDR (Managed Detection & Response):** Being proactive is everything in cybersecurity today. Our MDR takes an active approach built around threat profiling, threat defense, threat hunting, threat response, and threat intelligence and is powered solely on the Microsoft Security suite of products. When paired with other Difenda Shield components, you get a powerful tool that uses data-rich insights to provide actionable outcomes enabling business relevant decisions.

• **Difenda Shield AVM (Advanced Vulnerability Management):** This highly advanced and automation-driven platform continuously monitors, detects, and remediates vulnerabilities and configuration issues—providing real-time visibility into how vulnerabilities impact your organization, building detailed asset databases, understanding how to best prioritize vulnerabilities, and highlighting what steps to take.

• **Difenda Shield GRC (Governance, Risk, & Compliance):** Having the best technology means nothing if you do not have the right foundation to support your people and processes. Difenda Shield GRC gives organizations the essential cybersecurity foundation they need to drive the required frameworks and compliance to help eliminate fatigue within the security program.

• All of Difenda's capabilities form the basis of the Difenda Shield platform. This program is built upon the values of **confidentiality, integrity, and availability** to improve how we manage risks for our customers.

Today, Difenda is a Gold Security Services Partner for Microsoft with a growing presence in Canada, the USA, and Asia. With offices in all these regions Difenda is now enabling its customers across the globe in their fight against cybercrime.

Are you interested in learning more about the next generation of cybersecurity, MDR, and the new paradigm? Download our MDR eBook today.

About Difenda

Founded in 2008, Difenda is an industry-leading cybersecurity company with over a decade of deep expertise working in the most data-sensitive industries in the world. For the last five years, IDC Canada has recognized Difenda as a major cybersecurity service provider. As a proud Microsoft Gold Partner with two ISO 27001 certified Cyber Command Centers, SOC 2 Type 2 Compliance, along with other certifications and partnerships, Difenda has helped its customers build best-in-class, collaborative cybersecurity programs that empower their people, processes, and technology. Difenda is headquarter in Ontario, Canada with offices throughout Canada, the US, and Asia.

About the Author

Not long after completing his Bachelor of Engineering, Computer Science, Manoj Arora wrote his first mobile banking application at only 23. At 25, he was appointed as the youngest Cyber Security Officer for one of the largest banks in Asia. After traveling across the world, he had the opportunity to design cybersecurity infrastructure for some of the largest global organizations. Manoj currently heads Difenda, a top cybersecurity firm operating across North America and Asia. He has witnessed the evolution of the cybersecurity industry, the rapid push for digital transformations, and offers powerful insights into the future of cybersecurity.

Manoj Arora can be reached on LinkedIn or our website - be sure to check out his Tedx Talk.


Three-key encryption,
so you'll never have
ransomware face
ever again.
cryptoloc
The world's only three-key
data encryption technology.
Learn more at CRYPTOLOC.COM

The Skills to Propel Your Team's Cyber Security Defense

By Andrew Loschmann, Chief Operating Officer, Field Effect

Advancing your cyber security capabilities as you scale is an obvious need. But if you're resourced like many infosec departments, either very lean or running solo, it's always easier said than done. And as the pandemic throws more on your plate — there are often big expectations to meet, yet skilled talent and budget may be lacking.

If you're feeling like you're wearing multiple hats, rushing from one emergency to the next, or lacking the skills you need to move your department forward, you're not alone. Last year tested even the most experienced professionals. IT and security teams were presented new situations that took instant

priority — enabling remote workforces, securing cloud and video apps, setting permissions and policies, resolving user missteps, remediating COVID-19 threats, and more.

When your "to do" list changes instantly, it's tough to get back to implementing your security strategy. This is even more challenging without the right resources — yet, the fundamentals haven't changed. A scalable security plan requires technology that provides situational awareness as well as capabilities for effective remediation and tools to continually improve your security posture.

But technology is just half the battle. It's also the people on your team, whether in-house or outsourced, who help to create a strong threat defense.

The cyber security skills you need in your arsenal

IT environments are more complex and varied than ever before — and this requires as much visibility as possible across your network, systems, applications, and devices. To gain these insights, you not only need advanced, continuously improving technology, but human intelligence as well.

In fact, at the rate the cyber security industry evolves, you need security experts constantly ahead of the curve, educating themselves, and making sure they're staying on top of the latest threats and the sophisticated offensive techniques that pose a risk to your operations.

To put this into perspective, here are just a few cyber security roles needed for threat monitoring and detection:

- **Cyber Defense Analyst:** Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within IT environments with the goal of mitigating threats.

- **Cyber Threat Analyst:** Develops cyber indicators to maintain awareness of the status of highly-dynamic operating environments. Collects, processes, analyzes, and disseminates cyber threat and warning assessments.

- **Vulnerability Assessment Analyst:** Performs assessments of systems and networks within the network environment, identifying where those systems and networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

- **Cyber Defense Forensics Analyst:** Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system and network vulnerability mitigation.

While this is just a snapshot, each role requires extensive experience in cyber security and a combination of hard and soft skills — from software engineering and programming, computer and network forensics, network infrastructure management, and threat analysis to critical thinking, problem-solving, fast and strategic reaction, attention to detail, and the desire to learn — it's a long list, driven by the complexity of cyber security.

If you need more convincing of the human intelligence required to defend IT infrastructures, applications, devices, and users, look back at December 2020's massive SolarWinds supply chain attack, or the Exchange vulnerabilities patched by Microsoft in March.

In the case of SolarWinds, threat actors introduced a backdoor to Orion customers by modifying binaries supplied by SolarWinds in a supply chain attack that impacted more than 33,000 global customers. Following the installation of this backdoor, the attackers were able to gain access to networks of interest and leverage additional capabilities, such as compromising code signing certificates and forging authentication tokens — notoriously difficult to detect by even the most skilled security practitioners. The attack went undetected for months, enabling the threat actors to collect valuable intelligence from private companies, as well as U.S. agencies that included the Department of Homeland Security and the Treasury Department.

In the Microsoft Exchange incident, attackers actively exploited four zero-day vulnerabilities in Exchange Server. This left IT teams scrambling to patch systems and required incident response experts to develop tools and techniques to assess the impact and verify integrity following the compromise. During the event, security teams had to stay on top of the advice and guidance continuously updated from Microsoft and government agencies, while racing against malicious actors who were working to weaponize the exploits for ransomware.

These are both examples of security events that required deep expertise in cyber security forensics and incident response in order to act quickly and accurately to assess the impact to businesses.

The reality is, your immediate, or outsourced team, should have the cyber security training and expertise to understand attack techniques, threat behavior, the scope and severity of each new threat as it arises, the potential impact to your organization, and how to react quickly and effectively to mitigate active threats or risks. Teams should also bring the skills to evaluate and manage the technologies powering an organization's threat defense — whether that is hands-on engineering and software development or hiring outsourced experts that add this value.

The cyber skills gap

Every aspect of an effective cyber defense requires multiple and distinct roles, yet few small and mid-size businesses have the budget or cyber security knowledge and skills to build, manage, and invest in a team of in-house cyber security experts.

And that often results in job requisitions for security analysts or infosec professionals that don't fully capture all the responsibilities of the function. Or worse, a long list of IT and security requirements for just one position.

Talent to fill cyber security roles is also tough to find. As an industry, we're still facing a monumental skills gap — with research projecting that this year, there may be as many as 3.5 million unfilled cyber security jobs globally.

For just a few in-demand roles, the salaries and benefits alone could translate to multiple six figure positions — but more critically, it may be hard to source skills for even one of these.

Rethink your security defense

When applying the right skills and technologies for a strong cyber defense, it's key to look for the innovative solution providers that have the cyber expertise under their belt or have hired experienced cyber professionals and have continual training in place — or the service providers with security knowledge that are working with market innovators.

So if your cyber security strategy isn't giving you time back and improving your security, or you've outsourced your threat defense and are still overwhelmed with your 'to do' list, it's time to rethink your cyber security defense.

About the Author

Andrew Loschmann, Chief Operating Officer, Field Effect Software, Inc. Andrew Loschmann led five years of research and development efforts to bring Field Effect's sophisticated suite of Covalence threat monitoring and detection and Cyber Range simulation and training platforms, as well as other services, to the global market. Andrew brings a 20-year background building and managing IT security products and programs, including 13 years in government/defense, as well as security policy development within the Government of Canada's Privy Council Office and contributions to Canada's Cyber Security Strategy. His technical background includes development of software and systems, and cyber security analytics, as well as leading incident detection and response teams.

Andrew can be reached online at (EMAIL, TWITTER, etc..) and at our company website, https://fieldeffect.com/

MAKE SURE YOU'RE LEVERAGING MICROSOFT SECURITY!

Things have changed. Difenda will help maximize your Microsoft security investments through technology consolidation and provide a modular approach to provide a clear view of your cybersecurity landscape through a single pane of glass.

See the difference a personalized approach to cybersecurity makes work with a partner thats focused on you.

DIFENDA

CONTACT A DIFENDA SECURITY EXPERT TODAY

What Some Forget in Security – The Customer

By Timothy Liu, CTO & Cofounder, Hillstone Networks

For decades, security companies and experts, myself included, have pushed the mantra “Security first.” We prided ourselves in studying and predicting the evolution of threats within an industry. Those in the industry worked hard to be in front of those threats with sophisticated and new technology. The industry grew exponentially in anticipation that corporations big and small would build their business with security as a primary priority in mind.

It didn’t happen.

Instead, organizations were pummeled with breaches while corporate and government reputations took the hits. Not one industry or field was considered full proof. Instead, money was spent on security solutions that just ended up being band aids for the issues. Full, expensive security bundles were and continue to be purchased yet not fully implemented. It begs the question – where do we, as a security industry fall down? Believe it or not, it has little to do with the technology. It’s my belief that most security providers have a huge blind spot. Security providers fail to do what every other successful company does – listen to our customers.

It’s that simple. We need to be an industry that puts customer service first.

Most security companies have the simple mantra of “if you build it, they will come.” Security providers often fall into an echo chamber, insisting that their expertise within security outweighs the need to take customers opinions, wants and needs into account.

Customers don’t always need expensive solutions or platforms. In fact, it’s my belief that pushing unnecessary products will turn customers off to security as a whole, making the job of defending their systems even harder. We learned this very early at Hillstone Networks. Rather than focus on selling myriad security solutions, we needed to focus on what our customers wanted. What were their pain points? How can we keep them as safe as possible within the confines of budgets and size? We looked to be partners with our clients and give them as must protection as possible. We finally took our own advice and put their needs ahead of ours.

With this new shift in priorities, what ended up happening was exactly what we had hoped for. We have deep relationships with our customers. Our specialized technology is widely recognized by industry experts. We are regularly recognized by our customers in Gartner’s Customer Choice survey which is one of our most coveted honors. By listening to our customers, we have shaped our technology to meet everyone’s needs. Is it perfect? By all means no – but it’s a start. It’s the first step into reshaping client/vendor relations and improving the way the industry must work.

It’s time for other security companies to step away from the echo chamber and truly hear the customer. It’s the only way we will all win this battle against the bad actors.

About the Author

Timothy Liu is a veteran of the technology and security industry for over 25 years. Mr. Liu is co-founder and Senior Vice President of Hillstone Networks, responsible for global marketing and sales. As CTO, he is also responsible for the company's product strategy and technology direction. Prior to founding Hillstone, Mr. Liu managed the development of VPN subsystems for ScreenOS at NetScreen Technologies, and Juniper Networks following its NetScreen acquisition. He has also been a co-architect of Juniper Universal Access Control. In the past, he has served key R&D positions at Intel, Silvan Networks, Enfashion and Convex Computer. Timothy can be reached online at zhu@hillstonenet.com and at our company website http://www.hillstonenet.com/

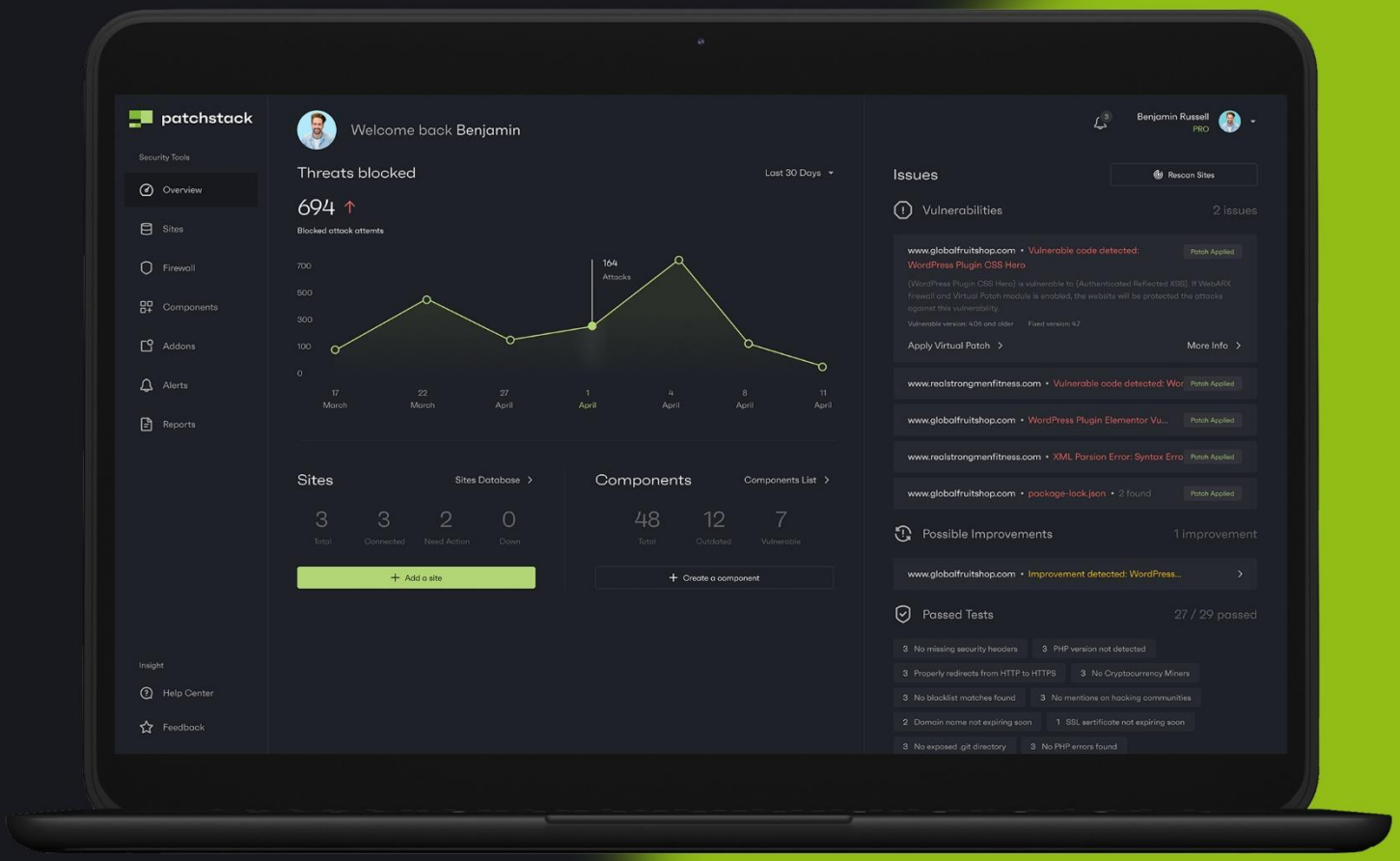
A NEW WAY TO KEEP YOUR SECRETS SAFE

www.freemindtronic.com

patchstack

Detect and patch third-party code vulnerabilities automatically

Patchstack connects bug bounties and community-driven security research with automated virtual patching to protect your websites.



Get Patchstack now from patchstack.com

The Security Challenge of Democratized Web

By Oliver Sild, the co-founder and CEO of Patchstack

Open-source adoption is growing rapidly. WordPress (a popular content management system) is a good example as it's now running more than 40% of the websites online.

The growth behind WordPress is largely caused by the large number of third-party plugins which allow its users to extend the functionality of the website.

Some of these third-party plugins have hundreds of thousands or even millions of active installations, which makes them an attractive target for malicious attacks.

Patchstack, an Estonian cyber-security company has taken an innovative approach to connect bug bounties and community-driven security research with automated virtual patching to solve that problem.

95% of security vulnerabilities in WordPress ecosystem originate from third-party plugins

Patchstack is maintaining a free to use vulnerability database for different website components which covers all security issues of WordPress core, themes and plugins.

When looking at all the vulnerabilities reported in 2020, 95% of the vulnerabilities originate from the third-party plugins and themes.

In 2020, we surveyed 338 digital agencies who specialize in website development and asked which threats are they most worried about. **The top 3 answers were:**

1) Lack of cyber security knowledge

2) Plugin and third-party code vulnerabilities

3) Blocking and preventing attacks

Anyone can create a new plugin and add it to the WordPress repository. While this is very convenient, it raises many concerns, since the skills of the plugin developers vary.

For the majority of the users, it's hard to tell which of the plugins are written poorly and which ones are not.

Businesses are becoming increasingly worried

Coming back to the survey we did in 2020, we also asked if the developers and digital agencies have witnessed a change in the number of hacking incidents.

We asked: "Have you seen a change in the number of attacks targeted against your websites?" - 157 out of 338 stated that they have seen an increase in the number of attacks against their websites and just 12 said that the numbers are decreasing instead.

We also asked if they are worried about the security of the websites and more than 73% of digital agencies and freelancers said **they are increasingly worried about website security**.

PS! This number was slightly higher (75%) among WordPress digital agencies and freelancers who use WordPress as their main platform.

Websites are being hacked

We also discovered that 25% of the responders have seen a hacked website in the past month prior to participating in the survey. This gives us a good understanding about the magnitude of the problem.

Websites are infected with malware and used to run further attacks against other websites and businesses. Hacked websites are often used to direct traffic to malicious sites, to steal credit card information and in some cases to even infect the visitor's computers.

Additionally, hosting phishing pages on hacked websites has become an increasingly popular tactic to steal credentials of third-party services.

Meanwhile, E-commerce websites are often targeted to inject websites with JavaScript based keyloggers to steal credit card details of online shoppers.

While gaining access to one small website might not be too valuable, exploiting a popular plugin can give the attacker access to hundreds of thousands or even to millions of sites with a single coordinated attack.

Community powered website security

The developer's community backing the open source projects like WordPress is strong and growing fast. Patchstack is now set on a mission to build a strong community of security researchers behind such popular projects too.

Patchstack ecosystem is combined of three services

Patchstack Platform - A SaaS product to automatically detect and patch third-party code vulnerabilities within websites.

Patchstack Red Team - A bug bounty platform which is motivating independent security researchers to find vulnerabilities in plugins and other popular open-source web components.

Patchstack Database - A free and open vulnerability database that can be used to keep up to date with the latest vulnerabilities within the web app components (currently WordPress core, plugins, themes).

"Giving back to the community is very important to us and for that reason, we have decided to make the data publicly accessible to everyone. Everything our in-house researchers or Patchstack Red Team community reports will ultimately be accessible for free at Patchstack Database." - CEO & Founder of Patchstack - Oliver Sild

The company believes that only by working together can we make the open source truly secure.

About the Author

Oliver Sild, the founder and CEO of Patchstack is an Estonian cyber security entrepreneur who has been actively giving back to the community through it's NGO by organising hacking competitions, cyber security events and running a hackerspace in Pärnu, Estonia.

OliverSild
Email: oliver.sild@patchstack.com
Twitter: @oliversild
Website: https://patchstack.com/

Gartner peerinsights customers' choice 2021™

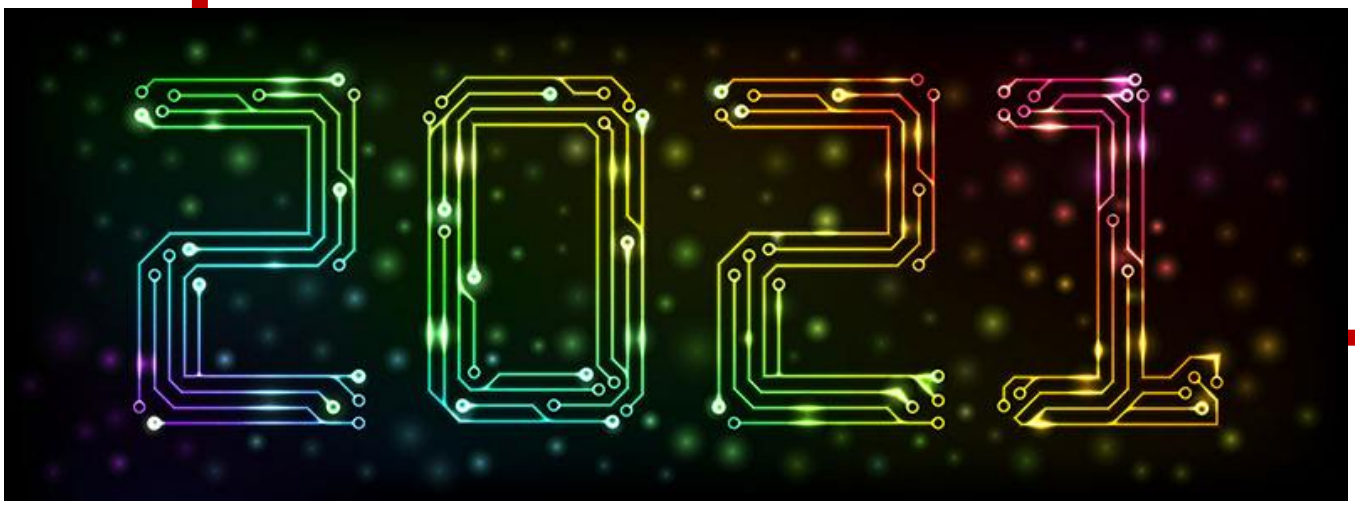
Gartner Peer Insights
Customers' Choice
Network Firewalls

Hillstone NETWORKS

What You Need to Know About Protecting Active Directory, the Attack Vector of Choice in 2021

Advanced threats are moving fast and have their eyes set on Active Directory

By Carolyn Crandall, Chief Security Advocate, Attivo Networks



Regardless of whether a cyberteacher's initial compromise originates from phishing or by exploiting vulnerabilities, they all have one common waypoint in mind, the company's Active Directory (AD). It's a treasure trove of data, and it stores the critical information needed to elevate an adversary's privileges and advance their attacks. Unfortunately, AD is complex and typically has legacy policies, overprovisioning, and entitlement creep, issues stemming from disjointed growth, turnover, and M&A. This all makes monitoring for bad amongst good activity very hard to detect. Sadly, the loss or misuse of domain control can be devastating, as seen in the recent SolarWinds, Microsoft, FireEye, and other high-profile ransomware attacks. These incidents should serve as a megaphone for every CISO and CIO that protecting Active Directory must be a top priority.

Protecting Active Directory is multifaceted and isn't about doing only one thing well. It requires mitigating risks, hardening AD systems, and efficiently detecting live attacks. Because AD is also commonly managed across IT and security teams, this can add to its management complexity. Some of the top things that organizations can do to improve their AD security posture include implementing least privileges and tiered admin accounts with limited extra privileges. They can also collect audit logs and sending them to SIEMs or UBA systems to reactively find threats.

The downside of this approach is that reviewing logs can be very time-consuming to get right, and many SOC and SIEM instances do not ingest Active Directory and domain controller logsnatively. These tools are also prone to generating false alerts that noisy and tend to mute out the important ones. Perhaps the biggest challenge is that these tools are reactive and don't proactively identify AD vulnerabilities that create risks related to credentials or domain access from endpoints. They are also not designed for live attack detection and will typically surface issues well after the event happens. This after-the-fact detection is similar to alerting on a car crash after it's happened, which is, of course, not very helpful except for recovery efforts. Viewing logs can also miss critical attacks like password spraying, DCSync, DCshadow, and Golden ticket or silver ticket attacks.

Attivo Networks has led the industry in providing efficient and accurate threat detection for credential theft and lateral movement activity. The company has continued to lead in innovation around credential and Active Directory protection. These include new ways to conceal credentials and AD objects from attackers, reveal attack paths, and deliver automated methods to find vulnerabilities in AD that create risk or demonstrate that a live attack is underway.

In 2020, Attivo announced ADSecure that hides AD objects from attackers. In 2021, the company announced ADAssessor, which automatically completes over 200 exposure checks, identifies over 70 vulnerabilities, and continuously detects over 10 critical live attacks. These products create an unprecedented level of visibility and attack prevention that has simply not been seen in the market before. Some of the quotes from our early adopters include:

"When I found out about this, I was pretty shocked and a bit skeptical, but very excited with the outcome that, Hey, this actually solves a problem that I've been, been looking at for years and years and years." – VP Information Security & IT Risk, Real Estate Equities Firm

"I haven't seen a tool yet that provides this level of visibility in a way that's so usable." – VP Information Security & IT Risk, Real Estate Equities Firm

"We say that ADAssessor should be something everybody does because Active Directory is just so commonly abused by attackers." – – VP Information Security & IT Risk, Real Estate Equities Firm

"ADAssessor provides a necessary and critical visibility into directory services and is a key component to provide identity and directory assurance." - CISO, Large Food Retailer

"A tool like ADAssessor is very great for understanding what are those hygiene changes that need to occur that I think you'll see used for spotting changes." - VP of IT infrastructure, Data Intelligence Firm

"ADAssessor is really treading some ground that I haven't seen before in a tool." - VP of IT infrastructure, Data Intelligence Firm

"Should the ADAssessor be a default security control? I would definitely qualify that it's a very foundational product." - VP of IT infrastructure, Data Intelligence Firm

The time to value is almost instantaneous because the ADAssessor tool can improve Directory assurance programs by

- Finding weaknesses and misconfigurations across AD domains and forests
- Reducing the attack surface by eliminating excessive and unneeded privileges
- Detecting dangerous delegation that attackers can easily exploit
- Continuous testing & health scores
- Automated collection of information and dashboard viewing
- A streamlined dashboard that shows the domain, user, and device risks present in AD
- Reporting with substantiation

Some specific examples of exposures found include finding domain replication backdoors, skeleton key vulnerabilities, DCShadow attacks, Kerberos vulnerabilities, misconfigured Kerberos delegations, hidden Security Identifier (SID), and weak LDAP Configurations.

In addition to finding vulnerabilities overlooked due to resources, skills, and time, the ADAssessor makes deployment, understanding the risk, and remediation a snap. The solution installs on one endpoint per domain and doesn't require any special privileges to operate.

Assessments can run continuously and are viewable in the solution's dashboard. The UI provides a health score along with insights into domain, user, and device-level risks. Each finding comes with MITRE ATT&CK mappings, details on the attack, and steps to remediate the incident, making information sharing amongst teams easy and providing the evidence required for actionable responses.

In some circumstances, organizations can't easily address vulnerable paths. For these situations, pairing the ADSecure solution with ADAssessor can also be very powerful for live attack detection. Some of the attacks detected include:

- Kerberoasting attack detection/prevention
- Domain privileges enumeration
- Silver ticket and golden ticket attack detection
- DCSync, DCShadow attack prevention
- Hide critical groups, domain admins, enterprise admins, etc.
- Prevent "Shadow Admin" account discovery
- Hide Critical Servers such as Exchange, IIS Web Servers, MSSQLsvc

Organizations can also pair Attivo Threat Path technology to gain visibility from the endpoint. The solution provides topographical maps to easily view credential exposures, misconfigurations, and other risks that attackers can exploit to gain domain control.

Putting this all into action, here are a couple of key use cases.

- Creation or expansion of a company's Domain Assurance program, regardless of size or program maturity.

- ADAssessor addresses and simplifies the following Domain Assurance dependencies with continuous visibility to exposures, misconfigurations, and attacks targeting Active Directory. It can also extend and automate AD expertise, expanding the breadth of people who understand the organization's AD, automating processes for more in-depth assessment, and provides context to remediate vulnerabilities faster

- ADSecure also efficiently hides AD objects from attackers. When an unauthorized query comes into AD, the solution only returns fake information designed to lead them into a decoy that safely observes and collects the attacker's actions. ADSecure can also run-in alert-only mode.

- Ransomware mitigation is another prevalent use case for Active Directory protection. Here, there are 3 ways to efficiently derail ransomware attacks using Attivo technology.

- The first is to hide the data they seek. With Attivo's unique DataCloak function, attackers cannot see or access the files, folders, mapped and removable drivesthey seek.

- Next, stand up fake data that will show instead of the real information. When the attacker attempts to engage with the fake data, a high interaction engine occupies the attacker, providing distraction and time to isolate the infected system from the network.

- The third is preventing the attacker from gaining control of Active Directory, stopping them from gaining the privileges they need to distribute malware to other endpoints or using lateral movement techniques as part of their attack

- In each scenario, the Attivo solution captures the unauthorized commands and the processes that spawned them

Whether focusing on supply chain vulnerabilities and detecting backdoors, endpoint protection and stopping lateral movement, or preventing privilege escalation, the Attivo Active Directory protection suite of products helps achieve better security defenses and scales from endpoints to AD and the cloud. Advanced threats are moving fast and have their eyes set on Active Directory. With these tools, organizations gain the power to stop them in their tracks. Contact Attivo at www.attivonetworks.com for a demo or to get pricing. An Active Directory protection checklist is available here.

About the Author

Carolyn Crandall is the Chief Security Advocate at Attivo Networks, the leader in preventing identity privilege escalation and detecting lateral movement attacks. She has worked in high-tech for over 30 years and has been recognized as a top 100 women in cybersecurity, a guest on Fox News, and profiled in the Mercury News. She is an active speaker on security innovation at CISO forums, industry events, and technology education webinars. Carolyn contributes regularly to security publications and co-authored the book Deception-Based Threat Detection: Shifting Power to the Defenders.

LinkedIn: https://www.linkedin.com/in/cacrandall/

Twitter: @ctcrandall

Evitoken Technology A New Way to Keep Secrets and Pass Them On

By Fabrice Crasnier, director of Research & Development department of FREEMINDTRONIC

Controlling the confidentiality of information is now an absolute necessity, as there are so many cyber malicious acts. We can cite among others acts such as phishing, stalking or ransomware. These so-called "cyber" threats alone represent approximately 75% of the infiltration techniques giving access to your confidential or personal data. All of these techniques have the same approach, which is identity theft. This mechanism allows an individual, or a machine, to impersonate someone or something else. The recipient thus deceived, lifts his natural mistrust to trust this ill-intentioned sender.

Protection techniques for transmitting confidential or personal data have been around for a very long time, as have signature mechanisms. They are most often based on asymmetric key algorithms, with strong encryption (RSA of 2048 or 4096 bits or even ECDSA). Unfortunately, if the model on which these encryption techniques are based is proven and ensures flawless security, its IT implementation is, for its

part, often undermined by man-in-the-middle attacks, or by elevations of law on information systems. These attacks, when identification or decryption relies only on one-factor authentication, allow the theft of encryption keys, and directly compromise the security of your data. To mitigate these threats, two-factor authentication (or 2FA) adds a layer of protection by either obtaining a unique code sent by SMS to your phone number, or by validating a request for it authentication (Google / Facebook), or through the use of authenticators which is increasingly recommended by security specialists.

Why use the EviToken Technology?

The purpose of EviToken technology is to secure secrets of different kinds, such as asymmetric keys (RSA), symmetric keys (AES) but also login information, PIN codes, account or bank card identifiers, cryptocurrency private keys, cryptocurrency wallet passphrases, cryptocurrency recovery phrases (SEED), etc. The EviToken secure safe is contained in a simple NFC card, not connected to a computer system. It communicates with the latter, on demand, via a near-field transmission protocol (NFC) which transmits data over an encrypted channel, built by EviToken. Secrets stored in the card are segmented and encrypted to make them physically inaccessible to cybercriminals. The EviToken secure safe is a real natural Air Gap component. Thus, apart from the case of data transmission, the architecture used has: no power supply; no security breach due to an increase in temperature (which makes it immune to malware such as "BitWhisper and Fansmitter"); no emission of sound signals, even those inaudible to the human ear and no emission of light or waves. Finally, to avoid a conflation with smart card-based systems, the support of EviToken technology does not require dedicated physical connection hardware with the digital system, nor does it have an operating system, which makes it insensitive to the introduction of malicious code as on a Java architecture. Like any electronic component, the EviToken secure safe can undergo invasive attacks which consist in using acids to expose the electronic circuit that will then have to be analyzed to try to understand the implementation of the secure secrets in multiple scrambled segments.

If EviToken technology provides security in a secure vault, what about the use of encryption keys to transport secrets over a secure channel?

In the context of two-factor authentication, we consider that you are the only one who can hold the second criterion of trust. This security measure traditionally allows, in case of failure, not to trigger the secure transport of your data. However, this function is not intended to secure the transport, it is the role of the encryption protocol to perform this operation. Thus, if the encryption keys are compromised, the data could be compromised during a listen. Faced with this problem, EviToken directly integrates metadata trust criteria into its encryption keys, in order to secure the encrypted messages during their transport. Thus, even in the event of a compromise of the keys, decryption remains blocked by the trust criteria. With this in mind, why stop at two criteria of trust? In its basic version, EviToken offers nine trust criteria based on the possession of a third-party object, technical components (phone ID, barcode, password, geolocation or BSSID) but also environmental and specific components to the sender, or recipient, to make data compromise even more difficult.

A simple example, you want to send a confidential message containing your latest invention to a colleague in a hostile environment, with a high probability of compromise. You will therefore add non-digital trust criteria to your encryption key, to ensure its protection in the event of a compromise. The decryption of the message by the AES 256 symmetric key will only be accessible, by the digital tool, once the conditions related to the trust criteria have been met. If we base one of the trust criteria on a geolocation for example, the recipient must not only be in possession of an EviToken card, but also be

physically located at the location of geolocation defined in the trust criteria to decrypt the message. This location may be known to the recipient like a convention, but may also not be known. The trust criterion will then be transmitted to him as one of the authentication multi-factors, by SMS / QR Code / Photo or any other means.

If EviToken technology provides security in a secure safe, encryption of messages with trust criteria based on environmental components, technical or not, what about the transmission of keys for use in a space digital connected?

To secure end-to-end transmissions, several tools, used as gateways, such as smartphones or virtual keyboards, will be crossed. EviToken then builds encrypted channels, from the first communications between the EviToken card and the first NFC communication gateway, using an AES 128 symmetric pairing key. The latter will be replaced by a 256-bit AES symmetric key, with different trust criteria depending on the user's choice, when recording a secret. Communication with web browsers is achieved using 256-bit ECC ephemeral keys (X25519), to negotiate exchanges between the smartphone and the browser plugin, to insert website authentication, text decryption, etc. As for the transmission, from the smartphone, of texts, images or encrypted files, the encryption is carried out with a symmetric key AES 256 bits with trust criteria.

Why choose the EviToken technology?

Our goal is to better understand the feasibility of digital malicious acts through a **human approach** to attacks. Thus, if you do not physically have the EviToken card, or if you do not have access to it with a connection duration long enough to carry out an attack, it will be very difficult to compromise the safe, but it is quite obvious that «to the impossible no one is bound ". "However, this attack requires physical contact, it is no longer possible to hide behind anonymizers. Assuming that the encrypted message is sufficiently protected, with algorithms such as 2048 or 4096 bit RSA or even ECDSA, then it is necessary to look into the protection of the key. Indeed, this protection will remain true as long as the encryption and decryption keys remain secret. History of computer attacks shows certain difficulties in maintaining this assertion. It is therefore necessary to strengthen the protection of the keys, by accepting the compromise of the latter, while protecting the message during its transport. at best for this requirement, non-digital trust criteria, that is to say criteria known, held, observable or understandable by the recipient, are required for the decryption of the message and no longer of the key.

EviToken technology, by adding these trust criteria, changes the current paradigm of access to secrets. Thus, even if a secret, and more particularly a decryption key, were stolen, it could only be used if the trust criteria are met.

Based on the EviToken principle, **the new EviCypher technology**, which won the 2021 gold medal for international inventions from Geneva, brings new innovations in the creation, management, integration and augmented intelligence linked to the use of trust criteria. A new chapter on this internationally patented invention on segmented key authentication is opening.

About the author

Fabrice Crasnier is the director of Research & Development departement of FREEMINDTRONIC. Freemindtronic, Andorran start-up designs and manufactures tailor-made solutions for its customers in the field of safety and cyber security of information systems and computer systems.

Fabrice is Associate Professor at Paul Sabatier University in Toulouse where he teaches cybercrime phenomena. He is at the origin of the creation of 3 forensic laboratories as head of forensic activities within the french police in Toulouse and within the SCASSI company. He has worked for 27 years in the judicial police, including 17 years following national and international cybercrime investigations. As a judicial expert since 2004 at the Court of Appeal of Toulouse, he has witnessed the delinquent transformation of cyberspace between 2000 and 2017. As a computer engineer, he has understood that the origin of cyberthreats is not always due to a defect in computer tools but more often to a misuse of these tools.

Fabrice can be reached online on Linkedin : https://www.linkedin.com/in/fabricecrasnier/

For more information, visit the company website at www.freemindtronic.com

How to Become Unattractive for Cybercriminals

Map, monitor and manage your attack surface to stay a step ahead

By Stijn Vande Casteele, Founder and CEO, Sweepatic

All organizations rely heavily on web presence to display their brand and/or products, reach their audience and streamline their processes. They deploy assets connected to the internet to achieve these goals. The benefits of the cloud, marketing websites and online services are obvious, but there are risks associated with any online presence. So, it becomes important to evaluate to what extent your organization is at risk of an attack by cybercriminals. That starts with understanding what your online

presence consists of, also known as your attack surface. How can you make your attack surface as small, flexible and secure as possible?

The Sweepatic Platform helps you strengthen the cyber resilience of your organization by not giving cybercriminals a real chance. People with malicious motivations will not be able to access your information if your “cyber doors” are closed. How can you approach that in concrete terms?

1. Be aware of your attack surface

Only when you understand the breadth and depth of your online presence you can really evaluate the risks your organization runs. An attack surface changes and grows continuously, which makes it hard and complex to have an up-to-date overview in real time.

For example, the Sweepatic Platform automatically and exhaustively scans the attack surface for vulnerabilities or CVEs (Common Vulnerabilities and Exposures). Sweepatic verifies email security settings which will prevent fraudulent or phishing emails sent in the name of an organization. Websites are verified against a list of configuration and encryption best practices. New cloud-based applications deployed with default and insecure settings are detected within days.

By keeping an eye on your attack surface, such risks can be avoided. The Sweepatic Platform discovers the full extent of your attack surface 24x7 and assesses in which areas you can remove targets for cyberattacks. You can slim down your attack surface in three concrete ways:

2. Websites and domain names

Keep an up-to-date view of which hosts your organization uses and manage them efficiently. You do this by updating your configurations, keeping an eye on which web applications are running and carefully handling where exactly you store and share confidential information. This provides you with an overview of which internet-facing assets - that no longer serve a business justification - to take offline or of where precisely you can improve your attack surface security.

After all, what is not there, cannot be hacked.

3. External providers

Nowadays, not all IT passes through or is managed by the IT department, let alone IT security. Are you aware of what is put online? Do you know exactly which external providers your organization uses? Not only is it safer to limit this group, it will likely save you monthly subscription fees as well.

4. Shadow IT

Shadow IT refers to the digital parts of an organization that people do not know about. This is caused by rapid digitization or due to inaccuracies during updates and adjustments. Shadow IT can add to costs and create an insecure cluster of online traces that can lead cybercriminals to your organization.

5. Increase your resilience through attack surface hygiene

The Sweepatic Platform provides visibility, tracks your digital assets, and analyzes issues in your attack surface by priority. Primary domains, subdomains, IP addresses, subnetworks, DNS records and locations are discovered and analyzed structurally and systematically. This way you will quickly discover dubious and/or unknown elements of your digital footprint.

6. Tackle risks in a smart way

You can get started reducing your risk right away with the actionable information that the Sweepatic Platform provides. In addition, implementing following approaches in your organization helps you build cyber resilience in a sustainable way.

7. Understanding

To thoroughly understand your attack surface, it is not enough to perform a one-time exercise. An attack surface and its risk exposure changes every day; technologies can become outdated, website certificates can expire, etc. Keep an eye continuously and in a structured way to ensure a real-time overview of all hosts and web applications that you use, for example.

8. More automation

Many cyber security tasks are repetitive. Rely on technology, such as machine learning algorithms, to perform these types of tasks. Less human error, speed and more scale are just some of the benefits of automated solutions, like the Sweepatic Platform. One of the biggest advantages is that you can use the talents of your scarce specialists to focus on other tasks to make your organization stronger in other ways.

9. Less complexity

By keeping an eye on your attack surface, you can continuously assess where to slim down your organization digitally and to simplify systematically. Keep asking yourself the question: "How can we

renew in a way that is safe, efficient and sustainable?". The Sweepatic Platform supports this by giving you the insights that help you stay in control.

10. Get started with Sweepatic

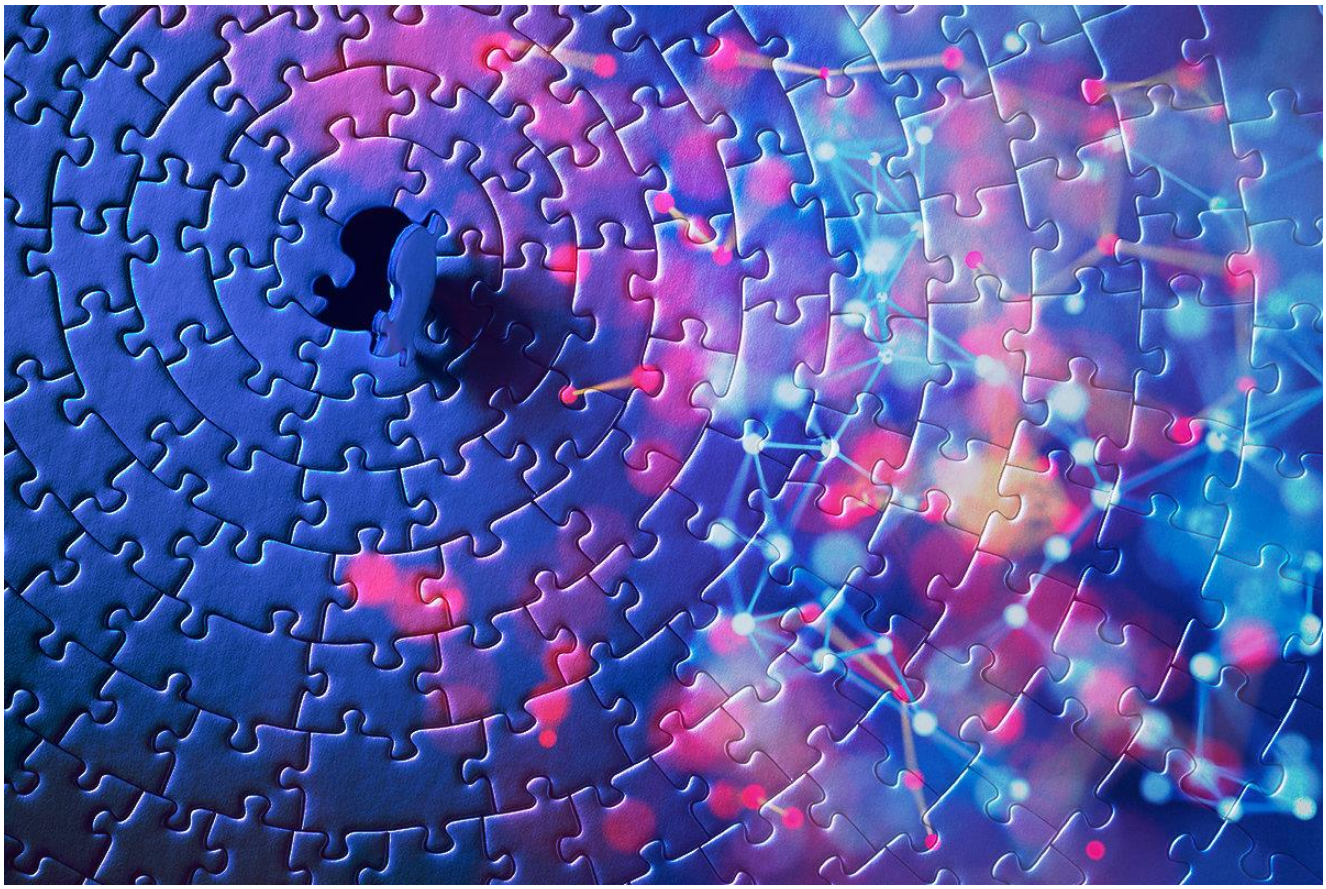
Contact us and we will help you get started right away. With a personalized demo you will get a first impression of the security and online presence of your company. We will tell you more about which concrete steps you can take and which are priority actions.

About the Author

Stijn Vande Casteele is the Founder and CEO of Sweepatic. He is an entrepreneur and seasoned cyber security professional with 19 years of experience. Stijn gained industry recognition based on his business insights and by coaching and steering several teams in successfully creating, delivering and operating enterprise enabled cyber security solutions for large organizations like NATO, BNP Paribas, Proximus and Deloitte. He is now fully focused on successfully scaling Sweepatic into a renowned cyber security business. Stijn can be reached online at www.linkedin.com/in/ictsecurity/ and at our company website www.sweepatic.com.

Why XDR is Not Enough

By Guy Rosefelt, Security CMO, Sangfor Technologies



What is XDR?

One of the latest trends in cybersecurity is Extended Detection and Response, more commonly known as XDR. Although originally defined by Palo Alto Networks as a key capability, other security vendors have released some type of XDR functionality and of course all define and approach it differently. Gartner defines XDR as "…a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components." Oddly, that sounds a lot like Security

Information Event Management (SIEM) with the addition of response capability. And that is the key point. Unlike SIEM, XDR does not only identify an incident, but it also has an automated response to it.

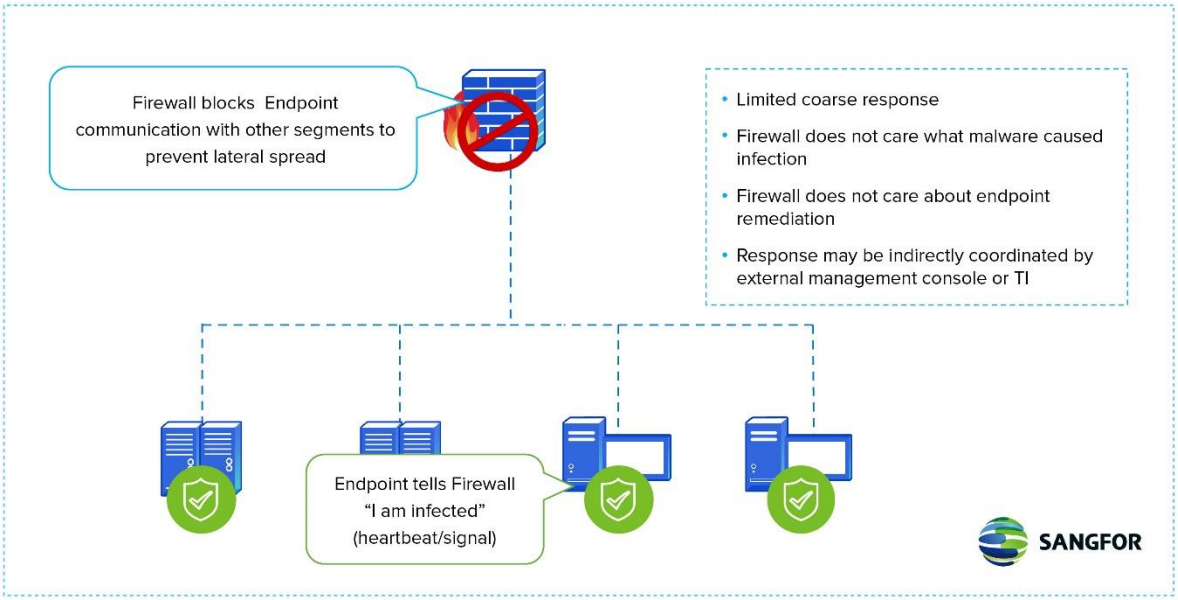
Most vendors with XDR are promoting integrating their security products together to build a more coordinated response. The reality is most XDR tries to integrate endpoints and networks together using endpoint detection and response (EDR) and next generation network firewalls (NGFW); the idea being EDR can tell the firewall what to block, such as malware command & control (C&C) communications.

Why XDR is Not Enough

So, as grand as the concept of XDR is, it is rather limited for several reasons:

- **XDR is usually one way**

In most XDR solutions, the EDR can send information to the firewall to trigger a response but the firewall does not normally send information to the endpoint to respond to a threat. For example, and endpoint can tell the firewall it is infected by malware and the firewall can block all communications from that endpoint. But the firewall, when seeing suspicious traffic, cannot ask the endpoint to run a scan to see if it is infected.



- **XDR response is not granular**

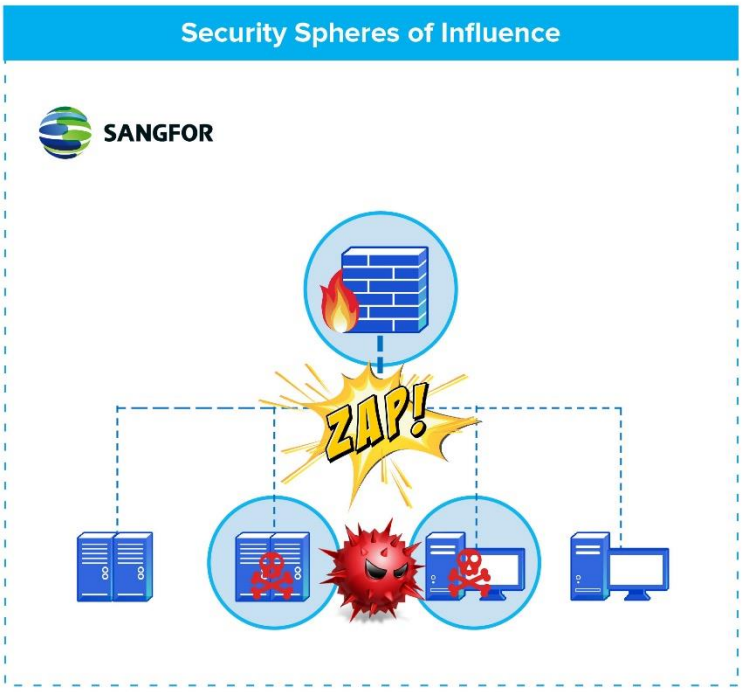
Normally, EDR will tell the firewall that the endpoint is infected. But what malware was detected or what ports the malware uses for C&C are not communicated. So, the firewall will block all communications from the endpoint, effectively isolating it from other network segments or the internet. But that would not be good if the endpoint were an ecommerce server generating revenue.

- **Response time slowed due to indirect communications**

As exciting as integrating EDR and NGFWs together sounds, the EDR and NGFW may not directly communicate with each other. Instead, communications and response instructions are routed through a management or threat intelligence (TI) platform. This indirect communication could impact how long it takes for a response to be initiated.

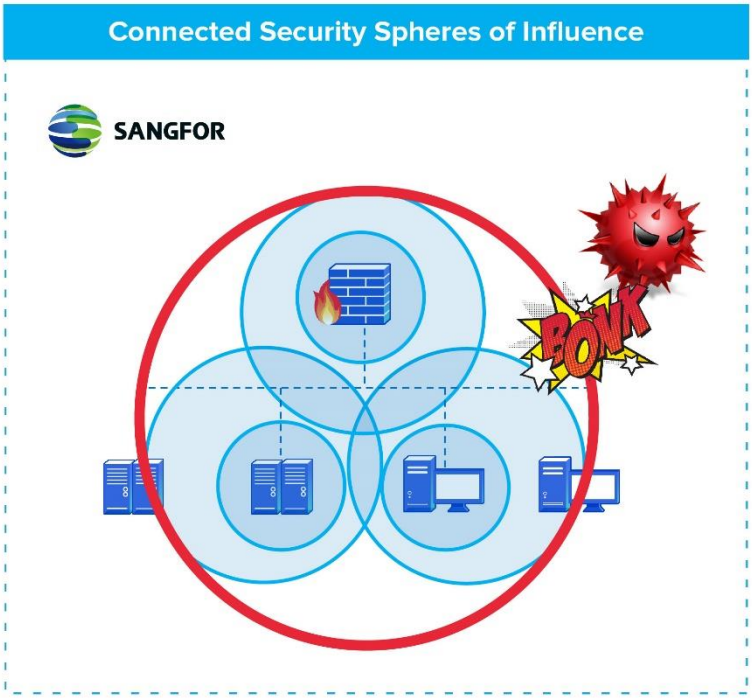
- **XDR does not close gaps between products**

All security products have a sphere of influence or area domain that they protect. NGFWs protect communications between networks. EDR protects endpoint from malware. But malware is becoming more sophisticated and can exploit the gaps in coverage between networks and endpoints.



Ransomware is a prime example of malware that can defeat XDR. To date ransomware is the most successful malware to breach, infect and attack data in organizations of every kind all around the world. And every organization infected by ransomware had some type of EDR and NGFW. The ransomware attack in Sept 2020 at Saraburi Hospital illustrates this. The attack made all online patient data unavailable and patients were asked to bring in copies of their medical records and prescriptions during treatment.

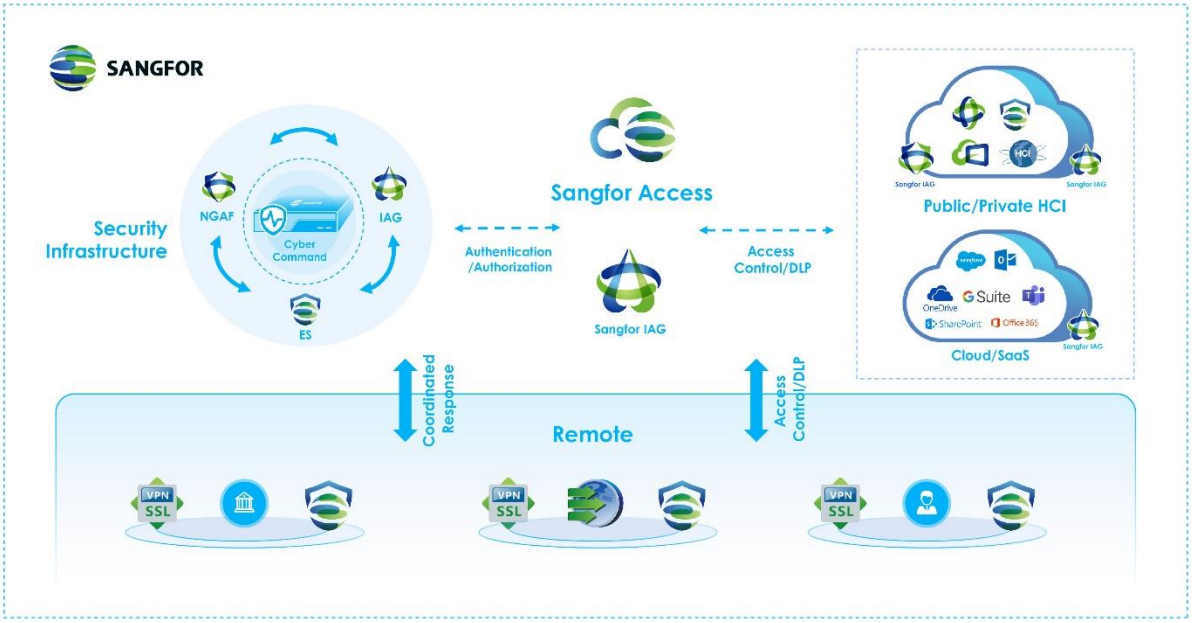
Adding Another 'D' to XDR



XDR as currently available is not enough. Better synergy between security products is needed to defend against upcoming AI enable malware. One way to improve synergy is to extend the spheres of influence of security products to close the gaps malware like ransomware can exploit. Enabling bi-directional direct communications between products creating closed feedback loops to better identify and more quickly defend and respond to threats is a must. Extending the spheres of influence for all products within an organization is important as customers have security solutions from more than one vendor and many really do not integrate well on their own.

Sangfor's Award Winning XDDR Security Framework

Sangfor's award winning eXtended Detection, Defense & Response (XDDR) strategy has implemented direct bi-directional communications long before XDR. And bi-directional communications are not just between the Sangfor NGAF network firewall and Endpoint Secure endpoint protection, but across all Sangfor security and cloud product lines. XDDR extends threat response beyond Sangfor products using the Cyber Command threat detection platform to integrate 3rd-party products.



Cyber Command correlates SIEM events, network traffic flow data, and endpoint protection data giving a 360-degree view of threats and risks in an organization. Multiple advanced AI models, cloud sandboxing, and direct response orchestration all contribute to XDDR's enhanced ability to coordinate and automate threat response across all products integrated into XDDR delivering true layered defense-in-depth even in hybrid cloud environments.

About Sangfor Technologies

Sangfor Technologies is an APAC-based, global leading vendor of IT infrastructure solutions specializing in Network Security and Cloud Computing with a wide range of products & services including Next-Generation Firewall, Internet Access Management, Endpoint Protection, Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, SASE, SD-WAN, and many others.

Sangfor takes customers' business needs and user experience seriously, placing them at the heart of our corporate strategy. Constant innovation and commitment to creating value for our customers help them achieve sustainable growth. Established in 2000, Sangfor currently has 7,500 + employees with more than 60 branch offices globally in exciting locations like Hong Kong, Malaysia, Thailand, Indonesia, Singapore, Philippines, Vietnam, Myanmar, Pakistan, UAE, Italy, etc.

Visit us at www.sangfor.com or send us an email to marketing@sangfor.com to learn more about Sangfor's Security solutions, and let Sangfor make your IT simpler, more secure and valuable.

About the Author

Guy Rosefelt, Security CMO of Sangfor Technologies. Guy previously served as the Director of Threat Intelligence & Web Security Product Management for NSFOCUS and with over 30 years experience in sales engineering, technical product design, technical marketing, business development, auditing & risk assessment for government, military and commercial companies worldwide - Guy is a leader and groundbreaker at the crux of a dynamic cyber-security industry.

Guy can be reached online at guy.rosefelt@sangfor.com and at Sangfor website https://www.sangfor.com/.

WELCOME TO ALLEGISCYBER CAPITAL

EARLY STAGE VENTURE CAPITAL INVESTMENTS IN CYBERSECURITY

ALL CYBER. ALL THE TIME.

We're a battle-tested team. We do one thing. Build great Cyber Security companies. Investing in cybersecurity isn't for newcomers – it requires years of experience, extensive contacts, deep knowledge and proven operational know-how.

THE ALLEGISCYBER CAPITAL ADVANTAGE

DATATRIBE + ALLEGISCYBER CAPITAL

TELL ME MORE

CYBER CRIMINALS

DON'T GIVE A $#!T:

- About your project's scope.
- It's managed by a third party.
- It's a legacy system.
- It's "too critical to patch."
- About your outage windows.
- About your budget.
- That you've always done it that way.
- About your go-live date.
- It's only a pilot/proof of concept.
- About non-disclosure agreements.
- It wasn't a requirement in the contract.
- It's an internal system.
- It's really hard to change.
- It's due for replacement.
- You're not sure how to fix it.
- It's handled in the Cloud.
- About your Risk Register entry.
- The vendor doesn't support that configuration .
- It's an interim solution.
- It's [insert standard here] compliant.
- It's encrypted on disk.
- The cost-benefit doesn't stack up.
- "Nobody else could figure it out."
- You can't explain the risk to "The business."
- You've got other priorities.
- About your faith in the competence of your internal rules.
- You don't have a business justification.
- You can't show return on investment.
- That it's supposed to be "Air Gapped."

But we do, and we're here to help!

SCADAfence

The Most Comprehensive
OT & IoT
Cyber Security Platform For
Critical Infrastructure &
Enterprises

www.SCADAfence.com


FIELD EFFECT™
We solved cyber security.
You're welcome.
Meet Covalence: the single source of protection for your entire IT ecosystem — endpoints, network and cloud. Powerful enough to protect entire countries, yet tailored for small and medium businesses like yours.
FIELD EFFECT
COVALENCE
fieldeffect.com/covalence

NETWORK SEGMENTATION · VIRTUAL PATCH · TRUST LIST

txone-networks.com

At TXOne Networks, we specialize in resilient, ironclad cybersecurity solutions for ICS environments. We do this through three key technologies that our researchers are constantly improving: network segmentation, virtual patching, and trust lists. By breaking the network up into smaller, easily-defensible segments based on work intention, by providing virtual patching to create a defensive shield around vulnerable legacy or unpatched assets, and by using trust listing to create a simple, zero trust-based system of access privileges, our solutions prioritize your availability and keep the operation running.

Award Winners

Welcome to the Cyber Defense Global InfoSec Awards for 2021

Cyber Defense Awards in conjunction with Cyber Defense Magazine is pleased to announce the winners of our prestigious annual Global Infosec Awards, now in their 9th year, here at the RSA Conference 2021. There are 3,200 cybersecurity companies in the world and the number is still growing. Our judges determined that roughly 10-15% deserve these prestigious awards in various categories, with a few we might add shortly after the show because of time constraints - it's exciting to share all these winners at https://cyberdefenseawards.com/ where the winners list is always up to date.

I've interviewed some of these winners in his https://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, we've done some exciting one-hour webinars with a select group at https://cyberdefensewebinars.com/, available on demand any time.

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, and many 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

SailPoint Market Leader Access Control

Safe-T Hot Company Access Control

Sphere Cutting Edge Access Control

vArmour Next-Gen Access Control

Account Takeover Protection

NuData Security, a Mastercard company Most Innovative Account Takeover Protection

Active Directory Security

Attivo Networks Hot Company Active Directory Security

Cion Systems Inc. Next-Gen Active Directory Security

Advanced Persistent Threat (APT) Detection and Response

BedRock Systems Inc. Editor's Choice Advanced Persistent Threat Detection and Response

SECUINFRA GmbH Best Product Advanced Persistent Threat Detection and Response

Group-IB Market Leader Advanced Persistent Threat Detection and Response

ARIA Cybersecurity Cutting Edge Advanced Persistent Threat Detection and Response

Cyber Defense InfoSec Awards for 2021

Anti-Malware

Ericom Software Best Product Anti-Malware

Anti-Phishing

Ericom Software Most Innovative Anti-phishing

Inspired eLearning, LLC. Cutting Edge Anti-phishing

IRONSCALES Hot Company Anti-phishing

KnowBe4 Market Leader Anti-phishing

OnDMARC by Red Sift Next-Gen Anti-phishing

SlashNext Editor's Choice Anti-phishing

API Security

Salt Security Most Innovative API Security

Application Digital Resiliency Solution

A10Networks Most Innovative Application Digital Resiliency Solution

Application Security

Checkmarx Market Leader Application Security

Digital.ai Hot Company Application Security

ForAllSecure Publisher's Choice Application Security

Denim Group Editor's Choice Application Security

HUMAN Most Promising Application Security

Imvision Next-Gen Application Security

Security Compass Most Innovative Application Security

vArmour Editor's Choice Application Security

Verimatrix Next Gen Application Security

WhiteHat Security Best Products Application Security

ZeroNorth Cutting Edge Application Security

Invicti Security Cutting Edge Application Security

Data Theorem Cutting Edge Application Security

Contrast Security Hot Company Application Security

Application-aware Workload Protection

Virsec Systems Hot Company Application-aware Workload Protection

Artificial Intellience

BlackBerry Market Leader Artificial Intellience

Artificial Intelligence and Machine Learning

Darktrace Holdings Limited Best Product Artificial Intelligence and Machine Learning

Egress Editor's Choice Artificial Intelligence and Machine Learning

IDology Next-Gen Artificial Intelligence and Machine Learning

Onfido Hot Company Artificial Intelligence and Machine Learning

Persona Publisher's Choice Artificial Intelligence and Machine Learning

Silobreaker Cutting Edge Artificial Intelligence and Machine Learning

LexisNexis Risk Solutions Cutting Edge Artificial Intelligence and Machine Learning

Attack Surface Management

Censys Publisher's Choice Attack Surface Management

Cyberpion Cutting Edge Attack Surface Management

Randori Editor's Choice Attack Surface Management

Sweepatic Most Innovative Attack Surface Management

Zentera Systems, Inc. Hot Company Attack Surface Management

Zscaler Next-Gen Attack Surface Management

Data Theorem Cutting Edge Attack Surface Management

Intelligent Waves Next-Gen Attack Surface Management

Attack Surface Protection

CyCognito Market Leader Attack Surface Protection

Cyber Defense InfoSec Awards for 2021

Authentication (Multi, Single or Two-Factor)

LexisNexis Risk Solutions Most Innovative Authentication (Multi, Single or Two-Factor)

Automated Detection Engineering

Anvilogic Most Innovative Automated Detection Engineering

Automated Forensic Malware Analysis and Hunt Tool

Cythereal Cutting Edge Automated Forensic Malware Analysis and Hunt Tool

Biometrics

iProov Next-Gen Biometrics

Nuance Communications, Inc. Most Innovative Biometrics

Blockchain Security

1Kosmos Next-Gen Blockchain Security

Breach & Attack Simulation

Cymulate Cutting Edge Breach & Attack Simulation

Keysight Technologies Hot Company Breach & Attack Simulation

Pcysys Most Innovative Breach & Attack Simulation

Picus Security Editor's Choice Breach & Attack Simulation

SafeBreach Inc Next-Gen Breach & Attack Simulation

Browser Isolation

Proofpoint Most Innovative Browser Isolation

BYOD

Hypori Inc. Cutting Edge BYOD

Central Log Management

Fluency Security Market Leader Central Log Management

Classification and Risk Mapping

Ground Labs Cutting Edge Classification and Risk Mapping

Cloud Access Security Broker (CASB)

Netskope Next-Gen Cloud Access Security Broker (CASB)

Cloud Backup

Arcserve Most Innovative Cloud Backup

Cloud Infrastructure Entitlement Management (CIEM)

Attivo Networks Hot Company Cloud Infrastructure Entitlement Management (CIEM)

CloudKnox Security Best Product Cloud Infrastructure Entitlement Management (CIEM)

Ermetic Hot Company Cloud Infrastructure Entitlement Management (CIEM)

Cloud Security

Anitian Editor's Choice Cloud Security

ARMO Publisher's Choice Cloud Security

Censys Cutting Edge Cloud Security

Lookout Most Innovative Cloud Security

Data Theorem Most Innovative Cloud Security

Netskope Best Product Cloud Security

Orca Security Most Promising Cloud Security

RedSeal Market Leader Cloud Security

Sonrai Security Next-Gen Cloud Security

ThreatModeler Software Inc. Most Innovative Cloud Security

Valtix Next-Gen Cloud Security Cloud Security

vArmour Hot Company Cloud Security

Volterra Cutting Edge Cloud Security

Zscaler Market Leader Cloud Security

Cloud Security Automation

Anitian Hot Company Cloud Security Automation

Cloud Workload Protection

ARMO Hot Company Cloud Workload Protection

ColorTokens Next-Gen Cloud Workload Protection

Confluera Editor's Choice Cloud Workload Protection

TrueFort Cutting Edge Cloud Workload Protection

Virsec Systems Most Innovative Cloud Workload Protection

Zscaler Best Product Cloud Workload Protection

Compliance

A-LIGN Market Leader Compliance

Anitian Next-Gen Compliance

Armor Most Innovative Compliance

Atlantic.Net Cutting Edge Compliance

BigID Best Product Compliance

Delphix Most Promising Compliance

Reciprocity Publisher's Choice Compliance

Spirion Editor's Choice Compliance

Strike Graph Hot Company Compliance

Tugboat Logic Cutting Edge Compliance

SberBank Most Innovative Compliance

Compliance Automation

Anitian Cutting Edge Compliance Automation

Consent & Preference Management

OneTrust PreferenceChoice Market Leader Consent & Preference Management

Container Security

NeuVector Most Innovative Container Security

Virsec Systems Hot Company Container Security

Continuous Controls Monitoring Platform

Panaseer Best Product Continuous Controls Monitoring Platform

Continuous Improvement and Optimization Services

CSIOS Corporation Hot Company Continuous Improvement and Optimization Services

Converged IAM

ILANTUS TECHNOLOGIES Most Innovative Converged IAM

Cyber Defense InfoSec Awards for 2021

Critical Infrastructure Protection

BedRock Systems Inc. Cutting Edge Critical Infrastructure Protection

QOMPLX Next-Gen Critical Infrastructure Protection

TXOne Networks, Inc. Most Innovative Critical Infrastructure Protection

Crypto Security

FREEMINDTRONIC Next-Gen Crypto Security

SpyCloud Cutting Edge Crypto Security

Cybersecurity Analytics

Cyberlumeneer Most Innovative Cyber Analytics

Cyber Insurance

Cowbell Cyber Editor's Choice Cyber Insurance

Cyber Threat Intelligence

CYFIRMA Most Innovative Cyber Threat Intelligence

Nucleon Cyber Best Product Cyber Threat Intelligence

Cybersecurity - Healthcare Practices

Alexio Corporation Market Leader Cybersecurity - Healthcare Practices

Cybersecurity Analytics

LexisNexis Risk Solutions Next-Gen Cybersecurity Analytics

Awake Security Most Innovative Cybersecurity Analytics

ChaosSearch Cutting Edge Cybersecurity Analytics

Spirion Hot Company Cybersecurity Analytics

Cybersecurity Artificial Intelligence

Axiado Corporation Editor's Choice Cybersecurity Artificial Intelligence

Traceable Editor's Choice Cybersecurity Artificial Intelligence

Darktrace Holdings Limited Editor's Choice Cybersecurity Artificial Intelligence

Cybersecurity Conference

Semperis Cutting Edge Cybersecurity Conference

Cybersecurity Discovery

Suridata.ai Most Innovative Cybersecurity Discovery

Cybersecurity Education - for Enterprises

Inspired eLearning, LLC. Hot Company Cybersecurity Education - for Enterprises

AwareGO Editor's Choice Cybersecurity Education - for Enterprises

Cybersecurity Education - for Small Business

Alexio Corporation Next-Gen Cybersecurity Education - for Small Business

Inspired eLearning, LLC. Most Innovative Cybersecurity Education - for Small Business

Cybersecurity Innovation

ANY.RUN Market Leader Cybersecurity Innovation

Cybersecurity Internet of Things (IoT)

Armis Best Product Cybersecurity Internet of Things (IoT)

Cujo AI Cutting Edge Cybersecurity Internet of Things (IoT)

Onward Security Corp. Hot Company Cybersecurity Internet of Things (IoT)

Cybersecurity Product Engineering Services

Sacumen Hot Company Cybersecurity Product Engineeering Services

Cybersecurity Research

BlackBerry Most Innovative Cybersecurity Research

Cybersecurity Startup of the Year

Anvilogic Editor's Choice Cybersecurity Startup of the Year

BedRock Systems Inc. Publisher's Choice Cybersecurity Startup of the Year

Cydome Security Cutting Edge Cybersecurity Startup of the Year

Cymptom Best Product Cybersecurity Startup of the Year

Cyolo Most Promising Cybersecurity Startup of the Year

DoControl, Inc. Most Innovative Cybersecurity Startup of the Year

Keyavi Data Corp. Next-Gen Cybersecurity Startup of the Year

Salt Security Hot Company Cybersecurity Startup of the Year

Security Scorecard Cutting Edge Cybersecurity Startup of the Year

Stellar Cyber Cutting-Edge Cybersecurity Startup of the Year

Cybersecurity Training

MITRE Engenuity Most Innovative Cybersecurity Training

Checkmarx Best Product Cybersecurity Training

Circadence Corporation Cutting Edge Cybersecurity Training

Fortinet Next-Gen Cybersecurity Training

Inspired eLearning, LLC. Editor's Choice Cybersecurity Training

KnowBe4 Market Leader Cybersecurity Training

PECB Most Promising Cybersecurity Training

RangeForce Market Leader Cybersecurity Training

Cybersecurity Training for Infosec Professionals

Infosec Inc. Best Product Cybersecurity Training for Infosec Professionals

Cybersecurity-as-a-Service (CaaS)

Allot Next-Gen Cybersecurity-as-a-Service (CaaS)

Cyvatar Cutting Edge Cybersecurity-as-a-Service (CaaS)

Data Center Security

HillStone Networks Market Leader Data Center Security

Data Governance

Egnyte Most Innovative Data Governance

Data Leakage Protection

Dasera Most Innovative Data Leakage Protection

Data Loss Prevention (DLP)

Altaro Software Next Gen Data Loss Prevention (DLP)

CoSoSys Cutting Edge Data Loss Prevention (DLP)

DTEX Systems Editor's Choice Data Loss Prevention (DLP)

GTB Technologies Best Product Data Loss Prevention (DLP)

Kingston Technology Market Leader Data Loss Prevention (DLP)

Data Protection

ICSDI - Ataguc Safe Next-Gen Data Protection

Data Recovery

Rubrik Publisher's Choice Data Recovery

SecureData Market Leader Data Recovery

Data Security

BigID Best Product Data Security

Cloudrise Cutting Edge Data Security

Concentric.ai Next-Gen Data Security

Imperva Market Leader Data Security

Keyavi Data Corp. Hot Company Data Security

PKWARE Most Promising Data Security

Protegrity Market Leader Data Security

RackTop Systems Most Innovative Data Security

Suridata.ai Publisher's Choice Data Security

Egnyte Next-Gen Data Security

Database Data Breach Prevention

Don't Be Breached Cutting Database Data Breach Prevention

DDoS Protection Scrubbing Center Solution

A10 Networks Next-Gen DDoS Protection Scrubbing Center Solution

Deception Based Security

Attivo Networks Market Leader Deception Based Security

Illusive Networks Most Innovative Deception Based Security

Deep Sea Phishing

Ericom Software Next-Gen Deep Sea Phishing

IRONSCALES Cutting-Edge Deep-Sea Phishing

Tessian Editor's Choice Deep Sea Phishing

Defensive Cyberspace Operations Team of the Year

CSIOS Corporation Publisher's Choice Defensive Cyberspace Operations Team of the Year

DevSecOps

Apiiro Cutting Edge DevSecOps

Denim Group Most Innovative DevSecOps

Security Compass Next-Gen DevSecOps

ZeroNorth Hot Company DevSecOps

Data Theorem Editor's Choice DevSecOps

Cyber Defense InfoSec Awards for 2021

Digital Executive Protection

BlackCloak, Inc. Editor's Choice Digital Executive Protection

Digital Footprint Security

Reflectiz Next-Gen Digital Footprint Security

Resecurity, Inc. Cutting Edge Digital Footprint Security

Spirion Editor's Choice Digital Footprint Security

Sweepatic Publisher's Choice Digital Footprint Security

Digital Rights Management

Fasoo Co., Ltd. Next-Gen Digital Rights Management

i2Chain, Inc. Most Innovative Digital Rights Management

Email Fraud Defense

Proofpoint Market Leader Email Fraud Defense

Email Security

RevBits LLC Most Innovative Email Security

Microsoft Cutting Edge Email Security

Email Security and Management

Datto Next-Gen Email Security and Management

Proofpoint Market Leader Email Security and Management

Cryptoloc Technology Editor's Choice Email Security and Management

Darktrace Holdings Limited Best Product Email Security and Management

IRONSCALES Cutting Edge Email Security and Management

OnDMARC by Red Sift Market Leader Email Security and Management

Zix Hot Company Email Security and Management

Perception Point Publisher's Choice Email Security and Management

Embedded Security

Enea Editor's Choice Embedded Security

Intrinsic ID Next-Gen Embedded Security

Lattice Semiconductor Cutting Edge Embedded Security

Encrypted Hardware

SecureData Most Innovative Encrypted Hardware

iStorage Best Product Encrypted Hardware

DataLocker Next-Gen Encrypted Hardware

Cyber Defense InfoSec Awards for 2021

Encryption

Cryptoloc Technology Next-Gen Encryption

Kingston Technology Market Leader Encryption

Quantum Xchange Best Product Encryption

RackTop Systems Cutting Edge Encryption

SafeLogic Editor's Choice Encryption

Zoom Video Communications, Inc. Hot Company Encryption

Endpoint Detection and Response (EDR)

RevBits LLC Most Innovative Endpoint Detection and Response (EDR)

Endpoint Security

Adaptiva Next-Gen Endpoint Security

BlackBerry Best Product Endpoint Security

DriveLock SE Market Leader Endpoint Security

Keeper Security Most Innovative Endpoint Security

McAfee Cutting Edge Endpoint Security

RevBits LLC Editor's Choice Endpoint Security

VMware Carbon Black Most Innovative Endpoint Security

Zscaler Market Leader Endpoint Security

SecPod Cutting Edge Endpoint Security

Microsoft Market Leader Endpoint Security

Enterprise Security

Anitian Publisher's Choice Enterprise Security

Anvilogic Cutting Edge Enterprise Security

Darktrace Holdings Limited Hot Company Enterprise Security

ThreatQuotient Editor's Choice Enterprise Security

vArmour Next-Gen Enterprise Security

ERP Data Security

Appsian Next-Gen ERP Data Security

ERP Risk Mitigation

Appsian Cutting Edge ERP Risk Mitigation

ERP Security

Onapsis Most Innovative ERP Security

Extended Detection and Response (XDR)

Beijing ThreatBook Technology Co. Ltd. Most Innovative Extended Detection and Response (XDR)

McAfee Market Leader Extended Detection and Response (XDR)

SANGFOR TECHNOLOGIES INC. Cutting Edge Extended Detection and Response (XDR)

Zentera Systems, Inc. Next-Gen Extended Detection and Response (XDR)

Microsoft Editor's Choice Extended Detection and Response (XDR)

Firewall

Untangle Inc Best Product Firewall

VMware Market Leader Firewall

Forensics

QuoLab Technologies Most Innovative Forensics

Fraud Prevention

LexisNexis Risk Solutions Hot Company Fraud Prevention

Arkose Labs Hot Company Fraud Prevention

Bolster Editor's Choice Fraud Prevention

Deduce Publisher's Choice Fraud Prevention

Group-IB Cutting Edge Fraud Prevention

Pindrop Most Innovative Fraud Prevention

Veriff Next-Gen Fraud Prevention

XTN Cognitive Security Best Product Fraud Prevention

Kount, An Equifax Company Next-Gen Fraud Prevention

SberBank Editor's Choice Fraud Prevention

Sumsub Hot Company Fraud Prevention

Global Managed Threat Detection and Response

Trustwave Market Leader Global Managed Threat Detection and Response

Go-To-Market Agency for Cyber Security Startups

Punch Most Innovative Go-To-Market Agency for Cyber Security Startups

Governance, Risk and Compliance (GRC)

Difenda Best Product Governance, Risk and Compliance (GRC)

Hardware Password Manager

FREEMINDTRONIC Most Innovative Hardware Password Manager

Hardware Security

Microsoft Best Product Hardware Security

Healthcare IoT Security

CyberMDX Cutting Edge Healthcare IoT Security

Medigate Most Innovative Healthcare IoT Security

IAM

Keeper Security Hot Company IAM

IAM Service

Herjavec Group Market Leader IAM Service

ICS/SCADA Security

Armis Next-Gen ICS/SCADA Security

Mission Secure Hot Company ICS/SCADA Security

TXOne Networks, Inc. Editor's Choice ICS/SCADA Security

SCADAfence Market Leader ICS/SCADA Security

Identity and Access Management

Axiad Hot Company Identity & Access Management

Centrify Editor's Choice Identity & Access Management

CloudKnox Security Market Leader Identity & Access Management

Devolutions Next-Gen Identity & Access Management

HID Global Cutting-Edge Identity & Access Management

Omada Publisher's Choice Identity & Access Management

One Identity Cutting Edge Identity & Access Management

OneLogin, Inc. Most Innovative Identity & Access Management

Optimal IdM Best Product Identity & Access Management

Ping Identity Most Promising Identity & Access Management

QOMPLX Most Innovative Identity & Access Management

Saviynt Next-Gen Identity & Access Management

Semperis Cutting Edge Identity & Access Management

SpyCloud Editor's Choice Identity & Access Management

Cyber Defense InfoSec Awards for 2021

Identity Management

Clear Skye Cutting Edge Identity Management

SailPoint Best Product Identity Management

Sonrai Security Next-Gen Identity Management

vArmour Cutting Edge Identity Management

Venafi Market Leader Identity Management

Identity Verification

Persona Cutting Edge Identity Verification

IDology Most Innovative Identity Verification

Regula Next-Gen Identity Verification

Veratad Technologies LLC Editor's Choice Identity Verification

Incident Response

Canopy Software Editor's Choice Incident Response

Endace Most Innovative Incident Response

Group-IB Next-Gen Incident Response

Logsign Cutting Edge Incident Response

OTRS Group Publisher's Choice Incident Response

QuoLab Technologies Hot Company Incident Response

SIRP Labs Limited Most Promising Incident Response

Cyber Defense InfoSec Awards for 2021

InfoSec Startup of the Year

Clayton Next-Gen InfoSec Startup of the Year

Hysolate Cutting Edge InfoSec Startup of the Year

King & Union Most Innovative InfoSec Startup of the Year

ShardSecure Editor's Choice Infosec Startup of the Year

Insider Threat Detection

Code42 Market Leader Insider Threat Detection

LinkShadow Best Product Insider Threat Detection

Insider Threat Prevention

DTEX Systems Next-Gen Insider Threat Prevention

Egress Cutting Edge Insider Threat Prevention

Gurucul Best Product Insider Threat Prevention

RackTop Systems Most Innovative Insider Threat Prevention

Integrated Risk Management

CyberSaint Security Editor's Choice Integrated Risk Management

Cyber Defense InfoSec Awards for 2021

Internet Filtering

SafeDNS, Inc. Market Leader Internet Filtering

Internet of Things (IoT)

SCADAfence Hot Company Internet of Things (IoT)

Intrusion Detection System

INTRUSION Most Innovative Intrusion Detection System

IT Automation and Cybersecurity

Coviant Software Next-Gen IT Automation and Cybersecurity

IT Vendor Risk Management (ITVRM)

LogicGate Cutting Edge IT Vendor Risk Management (ITVRM)

ProcessUnity Editor's Choice IT Vendor Risk Management (ITVRM)

Reciprocity Most Innovative IT Vendor Risk Management (ITVRM)

Malware Analysis

ANY.RUN Next-Gen Malware Analysis

ReversingLabs Best Product Malware Analysis

Malware Detection

Microsoft Most Innovative Malware Detection

Managed Detection and Response (MDR)

Alert Logic Best Solution Managed Detection and Response (MDR)

AT&T Cybersecurity Market Leader Managed Detection and Response (MDR)

Critical Insight, Inc Editor's Choice Managed Detection and Response (MDR)

CyberProof Cutting Edge Managed Detection and Response (MDR)

Deepwatch Market Leader Managed Detection and Response (MDR)

Difenda Next-Gen Managed Detection and Response (MDR)

eSentire Most Innovative Managed Detection and Response (MDR)

Field Effect Software, Inc Hot Company Managed Detection and Response (MDR)

Herjavec Group Market Leader Managed Detection and Response (MDR)

Netsurion Most Innovative Managed Detection and Response (MDR)

Orange Cyber defense Publisher's Choice Managed Detection and Response (MDR)

Managed Security Service Provider (MSSP)

CyberProof Cutting Edge Managed Security Service Provider (MSSP)

Deepwatch Best Product Managed Security Service Provider (MSSP)

Herjavec Group Market Leader Managed Security Service Provider (MSSP)

Neustar Inc. Market Leader Managed Security Service Provider (MSSP)

Orange Cyber defense Editor's Choice Managed Security Service Provider (MSSP)

Thrive Most Innovative Managed Security Service Provider (MSSP)

Avertium Next-Gen Managed Security Service Provider (MSSP)

Cyber Defense InfoSec Awards for 2021

MDR Service Provider

Proficio Most Innovative MDR Service Provider

Micro-segmentation

ColorTokens Next-Gen Micro-segmentation

Ericom Software Cutting Edge Micro-segmentation

Illumio Most Innovative Micro-segmentation

Safe-T Best Product Micro-segmentation

Zentera Systems, Inc. Editor's Choice Micro-segmentation

Mobile Application Security

Guardsquare Most Innovative Mobile Application Security

Mobile Endpoint Security

Guardsquare Next-Gen Mobile Endpoint Security

Lookout Market Leader Mobile Endpoint Security

MSSP

AT&T Cybersecurity Best Product MSSP

Netsurion Cutting Edge MSSP

QI-ANXIN Technology Group Inc Most Innovative MSSP

Multi-Factor Authentication

Axiad Hot Company Multi-Factor Authentication

LastPass Most Innovative Multi-Factor Authentication

WatchGuard Technologies Market Leader Multi-Factor Authentication

Network & Security Management

Untangle Inc Next-Gen Network & Security Management

Network Access Control (NAC)

Portnox Cutting Edge Network Access Control (NAC)

Network Detection and Response

Plixer Most Innovative Network Detection and Response

Cyber Defense InfoSec Awards for 2021

Network Security and Management

AlgoSec Cutting Edge Network Security and Management

ARIA Cybersecurity Most Innovative Network Security and Management

Endace Next-Gen Network Security and Management

Gigamon Market Leader Network Security and Management

LogRhythm Best Product Network Security and Management

Lookout Publisher's Choice Network Security and Management

Zero Networks Editor's Choice Network Security and Management

WatchGuard Technologies Hot Company Network Security and Management

Next Generation Firewall

HillStone Networks Most Innovative Next Generation Firewall

Open-Source Security

Patchstack Cutting Edge Open-Source Security

Xmirror Security Next-Gen Open-Source Security

Onward Security Corp. Next-Gen Open-Source Security

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

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

Packet Capture Platform

Endace Market Leader Packet Capture Platform

PAM for Cloud Infrastructure

CloudKnox Security Best Product PAM for Cloud Infrastructure

Passwordless Authentication

Aware, Inc. Best Product Passwordless Authentication

Axiad Most Innovative Passwordless Authentication

TruU Cutting Edge Passwordless Authentication

Veridium Next-Gen Passwordless Authentication

Pentesting-as-a-service (PtaaS)

Cobalt Next-Gen Pentesting-as-a-service (PtaaS)

PR Firm for InfoSec Companies

ARPR Publisher's Choice PR Firm for InfoSec Companies

LaunchTech Communications Hot Company PR Firm for InfoSec Companies

Lumina Communications Market Leader PR Firm for Infosec Companies

Privacy Management Software

IDX Editor's Choice Privacy Management Software

Spirion Next-Gen Privacy Management Software

TrustArc Cutting Edge Privacy Management Software

Privacy Research Solution

OneTrust DataGuidance Most Innovative Privacy Research Solution

Privileged Access Management (PAM)

Fudo Security Next-Gen Privileged Access Management (PAM)

RevBits LLC Best Product Privileged Access Management (PAM)

Privileged Account Security

Devolutions Most Innovative Privileged Account Security

Remediant Market Leader Privileged Account Security

Railway Cybersecurity

Cervello Cutting Edge Railway Cybersecurity

Ransomless Ransomware Solution

Stash Global Inc. Most Innovative Ransomless Ransomware Solution

Ransomware Protection of SaaS Data

Spin Technology, Inc. Next-Gen Ransomware Protection of SaaS Data

Ransomware Recovery Solution

Semperis Cutting Edge Ransomware Recovery Solution

Risk Management

CyberSaint Security Editor's Choice Risk Management

Reciprocity Cutting Edge Risk Management

RiskIQ Best Product Risk Management

RiskLens Next-Gen Risk Management

Runtime Memory Protection

Virsec Systems Best Product Runtime Memory Protection

SaaS Security

DoControl, Inc. Publisher's Choice SaaS Security

SaaS/Cloud Security

ANY.RUN Publisher's Choice SaaS/Cloud Security

Axis Security Editor's Choice SaaS/Cloud Security

Beijing ThreatBook Technology Co. Ltd. Cutting Edge SaaS/Cloud Security

Clayton Most Promising SaaS/Cloud Security

ColorTokens Publisher's Choice SaaS/Cloud Security

ExtraHop Next-Gen SaaS/Cloud Security

Iboss Market Leader SaaS/Cloud Security

Lightspin Hot Company SaaS/Cloud Security

ManagedMethods Cutting Edge SaaS/Cloud Security

Spin Technology, Inc. Next-Gen SaaS/Cloud Security

Webscale Editor's Choice SaaS/Cloud Security

Zscaler Best Product SaaS/Cloud Security

Anitian Most Innovative SaaS/Cloud Security

SD-WAN

HillStone Networks Cutting Edge SD-WAN

SecOps-as-a-service

Cyvatar Most Innovative SecOps-as-a-service

Secrets Management

FREEMINDTRONIC Next-Gen Secrets Management

Secure Coding: Developer Upskilling

Secure Code Warrior Most Innovative Secure Coding: Developer Upskilling

Secure Communications

BlackBerry Best Product Secure Communications

Secure Remote Access

Fudo Security Next-Gen Secure Remote Access

Secure SaaS Backups

Spin Technology, Inc. Most Innovative Secure SaaS Backups

Security Awareness Training

Infosec Market Leader Security Awareness Training

Proofpoint Editor's Choice Security Awareness Training

Security Company of the Year

Anitian Publisher's Choice Security Company of the Year

BlackBerry Market Leader Security Company of the Year

ColorTokens Hot Company Security Company of the Year

Darktrace Holdings Limited Market Leader Security Company of the Year

Egress Editor's Choice Security Company of the Year

eSentire Editor's Choice Security Company of the Year

Herjavec Group Most Innovative Security Company of the Year

Keeper Security Cutting Edge Security Company of the Year

Lookout Next-Gen Security Company of the Year

Raytheon Intelligence & Space Cutting Edge Security Company of the Year

ReversingLabs Next-Gen Security Company of the Year

SANGFOR TECHNOLOGIES INC. Most Promising Security Company of the Year

Zscaler Most Innovative Security Company of the Year

Security Governance, Risk and Compliance (GRC)

SCADAfence Market Leader Security Governance, Risk and Compliance (GRC)

Security Information Event Management (SIEM)

Devo Cutting Edge Security Information Event Management (SIEM)

Graylog Editor's Choice Security Information Event Management (SIEM)

LogRhythm Best Product Security Information Event Management (SIEM)

SECUINFRA GmbH Publisher's Choice Security Information Event Management (SIEM)

Securonix Most Innovative Security Information Event Management (SIEM)

Sumo Logic Next-Gen Security Information Event Management (SIEM)

Thrive Hot Company Security Information Event Management (SIEM)

Security Investigation Platform

Endace Next-Gen Security Investigation Platform

King & Union Cutting Edge Security Investigation Platform

Swimlane Most Innovative Security Investigation Platform

ThreatQuotient Best Product Security Investigation Platform

Security Project of the Year

BedRock Systems Inc. Most Innovative Security Project of the Year

SberBank Cutting Edge Security Project of the Year

Zscaler Editor's Choice Security Project of the Year

Cyber Defense InfoSec Awards for 2021

Security Ratings

Panorays Cutting Edge Security Ratings

RiskRecon Next-Gen Security Ratings

Security Software

Versa Networks Most Innovative Security Software

Security Team of the Year

SecurityMetrics Most Innovative Security Team of the Year

Bank of America Most Innovative Security Team of the Year

Security Training

Field Effect Software, Inc Best Product Security Training

Self-protecting Data Security

Cryptoloc Technology Cutting Edge Self-Protecting Data Security

Keyavi Data Corp. Next-Gen Self-protecting Data Security

SIEM

Logsign Most Innovative SIEM

Single Sign on

CionSystems Inc Best Product Single Sign on

SMB Cybersecurity

A-LIGN Editor's Choice SMB Cybersecurity

Defendify Best Product SMB Cybersecurity

Devolutions Next-Gen SMB Cybersecurity

Field Effect Software, Inc Most Innovative SMB Cybersecurity

JumpCloud Cutting Edge SMB Cybersecurity

Orange Business Service Publisher's Choice SMB Cybersecurity

Sectigo Most Innovative SMB Cybersecurity

TPx Most Promising SMB Cybersecurity

WatchGuard Technologies Market Leader SMB Cybersecurity

Zix Cutting Edge SMB Cybersecurity

SOAR

QI-ANXIN Technology Group Inc Best Product SOAR

Siemplify Next-Gen SOAR

SOC-as-a-Service

Netsurion Most Innovative SOC-as-a-Service

Performanta Cutting Edge SOC-as-a-Service

Proficio Best Product SOC-as-a-Service

Comtact Next-Gen SOC-as-a-Service

Software Composition Analysis

Checkmarx Cutting Edge Software Composition Analysis

GrammaTech Next-Gen Software Composition Analysis

Software Development Lifecycle Security

Clayton Cutting Edge Software Development Lifecycle Security

Telecoms Fraud Prevention

SpyCloud Next-Gen Telecoms Fraud Prevention

LexisNexis Risk Solutions Best Product Telecoms Fraud Protection

Third Party Risk Management (TPRM)

CyberGRX Best Product Third Party Risk Management (TPRM)

ProcessUnity Cutting-Edge Third-Party Risk Management (TPRM)

Reciprocity Most Innovative Third-Party Risk Management (TPRM)

Resecurity, Inc. Next-Gen Third Party Risk Management (TPRM)

Threat Intelligence

LexisNexis Risk Solutions Editor's Choice Threat Intelligence

Cobwebs Technologies Cutting Edge Threat Intelligence

Cyware Editor's Choice Threat Intelligence

Flashpoint Publisher's Choice Threat Intelligence

King & Union Most Promising Threat Intelligence

QuoLab Technologies Next-Gen Threat Intelligence

Resecurity, Inc. Cutting Edge Threat Intelligence

ReversingLabs Most Innovative Threat Intelligence

Silobreaker Next-Gen Threat Intelligence

ThreatQuotient Hot Company Threat Intelligence

Beijing ThreatBook Technology Co. Ltd. Best Product Threat Intelligence

Alert Logic Market Leader Threat Intelligence

Threat Modeling

ThreatModeler Software Inc. Most Innovative Threat Modeling

Token Based IAM

uQontrol Hot Company Token Based IAM

Unified Cloud Edge (UCE) Security

McAfee Market Leader Unified Cloud Edge (UCE) Security

Unified Threat Management (UTM)

WatchGuard Technologies Cutting Edge Unified Threat Management (UTM)

User Behavior Analytics

NuData Security, a Mastercard company Cutting Edge User Behavior Analytics

Vulnerability Assessment, Remediation and Management

Adaptive Shield Next-Gen Vulnerability Assessment, Remediation and Management

Pcysys Cutting Edge Vulnerability Assessment, Remediation and Management

SecurityMetrics Most Innovative Vulnerability Assessment, Remediation and Management

XM Cyber Best Product Vulnerability Assessment, Remediation and Management

SeureWorks Hot Company Vulnerability Assessment, Remediation and Management

SecPod Hot Company Vulnerability Assessment, Remediation and Management

Vulnerability Intelligence

Risk Based Security Cutting Edge Vulnerability Intelligence

RiskSense Most Innovative Vulnerability Intelligence

Silobreaker Editor's Choice Vulnerability Intelligence

Vulnerability Management

Denim Group Publisher's Choice Vulnerability Management

Difenda Most Promising Vulnerability Management

Intel Next-Gen Vulnerability Management

Kenna Security Cutting Edge Vulnerability Management

Pcysys Most Innovative Vulnerability Management

Skybox Security Next-Gen Vulnerability Management

RiskSense Next-Gen Vulnerability Management

Vulnerability Management (Operational Technology)

Industrial Defender Hot Company Vulnerability Management (Operational Technology)

Web Application Security

Fastly (Signal Sciences) Publisher's Choice Web Application Security

HUMAN Next-Gen Web Application Security

Invicti Security Next-Gen Web Application Security

Kasada Editor's Choice Web Application Security

Neustar Inc. Market Leader Web Application Security

Patchstack Cutting Edge Web Application Security

Penta Security Systems Inc. Most Innovative Web Application Security

Reblaze Hot Company Web Application Security

Reflectiz Most Promising Web Application Security

ThreatX Best Product Web Application Security

Wireless, Mobile, or Portable Device Security

Kingston Technology Most Innovative Wireless, Mobile, or Portable Device Security

WatchGuard Technologies Next-Gen Wireless, Mobile, or Portable Device Security

XDR – Extended Detection and Response

Confluera Cutting Edge XDR – Extended Detection and Response

Fidelis Cybersecurity Best Product XDR – Extended Detection and Response

Red Piranha Limited Next-Gen XDR – Extended Detection and Response

Stellar Cyber Most Innovative XDR – Extended Detection and Response

Zero Trust

Fudo Security Hot Company Zero Trust

Spotlight on Women in Cybersecurity

By Carolyn Crandall, Chief Security Advocate and CMO, Attivo Networks, Inc.

"There are a wide variety of roles for women in cybersecurity. Don't let any job description intimidate you, and if it feels like it is a stretch, all the better. Be who you want to be. Go for the job that you want to have. You've got this!"

I started my career in technology while still attending college. Going into high-tech was and wasn't something that I had given much thought to. At the time, I was obtaining a degree in electrical engineering and computer science. Why? Mainly because it seemed like a challenge, and I wanted to break down the perception that women couldn't do it. During this time, I don't recall ever hearing a murmur about cybersecurity.

Admittedly, I loved technology but was a terrible coder. I tended to overthink things. As luck would have it, I secured a part-time position as an assistant to a vice president of marketing at a computer manufacturer. In this role and throughout my career, I was exposed to endless innovation that brought technology from mainframes down to compute and storage that could easily be held in the palm of my hand. It has been truly fascinating, and it opened my eyes to the numerous jobs for women in technology.

Fast forward to today, I am truly honored to be recognized as a top woman in cybersecurity. I have worked for notable companies like Cisco, Seagate, Riverbed, and others that have given me fantastic experiences with technology and security. Attivo Networks, where I am the Chief Security Advocate and CMO, has provided me with an excellent opportunity to further my career in cybersecurity. Here, I heavily invest my time educating the market on solving business problems with innovations in cybersecurity technology. I am a frequent presenter, blogger, and writer; I have also been profiled in the Mercury News and have been a guest speaker on Fox News. My articles can be found in a variety of publications, and you can read the book I co-authored called Deception-Based Threat Detection: Shifting Power to the Defenders. I am also an advisor to the Santa Clara University Executive MBA program, where I support education and career development programs for our next generation of cybersecurity and technology leaders.

Cyber Defense InfoSec Awards for 2021

CEO of the Year

Tony Velleca CyberProof CEO of the Year

Kevin Gosschalk Arkose Labs CEO of the Year

Jay Chaudhry Zscaler CEO of the Year

Mr. Cesar Pie CSIOS Corporation CEO of the Year

Dr. Aleksandr Yampolskiy Security Scorecard CEO of the Year

Klaus Oestermann BedRock Systems Inc. CEO of the Year

Prakash Panjwani WatchGuard Technologies CEO of the Year

CISO of the Year

Mike Hamilton Critical Insight, Inc CISO of the Year

Ryan Weeks Datto CISO of the Year

CTO of the Year

Charles Eagan Blackberry CTO of the Year

Satya Gupta Virsec Systems CTO of the Year

Cybersecurity Strategist of the Year

Mr. Clinton Hackney CSIOS Corporation Cybersecurity Strategist of the Year

Cyber Defense InfoSec Awards for 2021

Security Expert of the Year

Caroline Wong Cobalt Security Expert of the Year
Stuart Reed Orange Cyber Defense Security Expert of the Year

Top Women in Cybersecurity

Aimei Wie Stellar Cyber Top Women in Cybersecurity

Alex Kobray Flashpoint Top Women in Cybersecurity

Anna Collard KnowBe4 Top Women in Cybersecurity

Alex Kobray TalaTek, a Cerberus Sentinel company Top Women in Cybersecurity

Stephanie Fohn NeuVector Top Women in Cybersecurity

Christina Luttrell IDology Top Women in Cybersecurity

Dr. Nicole Fern Tortuga Logic, Inc. Top Women in Cybersecurity

Ingrid Gliottone BlackCloak, Inc. Top Women in Cybersecurity

Leah Freiman ItCon Inc. Top Women in Cybersecurity

Lee Kappon Suridata.ai Top Women in Cybersecurity

Susanne Gurman Security Scorecard Top Women in Cybersecurity

Teresa Shea Raytheon Intelligence & Space Top Women in Cybersecurity

Vanita Pandey Arkose Labs Top Women in Cybersecurity

Michel Huffaker ThreatQuotient Top Women in Cybersecurity

Carolyn Crandall Attivo Networks Top Women in Cybersecurity

Nicola Jakeman Orange Cyber defense Top Women in Cybersecurity

Kimberly Sutherland LexisNexis Risk Solutions Top 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

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

Founder & Managing Partner

SEAN DRAKE

U.S.ARMY

"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