THE BLACK UNICORN REPORT

With David DeWalt, Robert Ackerman and Gary Miliefsky

and our newest judge, this year: Dr. Peter Stephenson

www.cyberdefenseawards.com

The Black Unicorn Report for 2021

Contents

What is a Black Unicorn?

In the venture capital industry, a unicorn refers to any tech startup company that reaches a $1 billion-dollar market value as determined by private or public investment.

The term was originally coined in 2013 by venture capitalist Aileen Lee, choosing the mythical animal to represent the statistical rarity of such successful ventures. Last year, CB Insights reported that the odds of becoming a unicorn — a company valued at $1 billion or more — was less than 1% for companies that had raised venture capital. In 2018, there were 47 tech companies in the US to reach this unicorn status, according to data provided by PitchBook.

In the cybersecurity industry, in 2019, Gary S. Miliefsky coined the term black unicorn as a cybersecurity company that has the potential to reach a $1 billion-dollar market value as determined by private or public investment.

The black unicorn awards are designed to help showcase companies with this kind of potential. Ultimately, the judging in our awards is tough and it's still up to those notable mentions, finalists and the winners to execute a flawless business model to reach this potential. It takes innovation, dedication, passion – the right team and the right cyber security solution, harmoniously executed to become a unicorn.

Our mission is to uncover future Black Unicorns and based upon the hard work of our judges and the entrants in our awards program, we think we've found them.

Let's not forget last year's winners: Armis, Checkmarx, Code42, Dragos, KnowBe4, ObserveIT, RedSeal, Remediant, ReversingLabs and XM Cyber, of which KnowBe4 has gone public for over $3B in value, exceeding our expectations.

We thank Robert Herjavec for his passionate support in kicking off the Black Unicorn Awards and helping us judge them in our first year. This year, our judges, and some information about them, follow. Our Judges for the Black Unicorn Awards this year are Gary S. Miliefsky, Dr. Peter Stephenson, Dr. David DeWalt and Robert R. Ackerman, Jr.

Now, let's introduce the Judges…

CYBER DEFENSE
MEDIA GROUP

The Global Source for Cybersecurity News and Information since 2012

Cyber Defense Media Group is on a non-stop mission of growth – to share daily infosec news, tips and knowledge you won't find anywhere else. With **over 10,000 searchable pages** of online content, **over 175,000 opt in email** recipients of which **more than 50,000 are CISOs and CIOs**, a **Top 3% global LinkedIn account** and newly launched platforms, each year, we are delivering on our promise. By the end of 2021 we will have reached ***5,000,000 unique online readers***, growing daily. Our platforms can be found at:

www.cyberdefensemagazine.com

www.cyberdefenseradio.com

www.cyberdefensetv.com

www.cyberdefenseprofessionals.com

www.cyberdefensewebinars.com

www.cyberdefenseawards.com

While we're in our 9th year of awards, 2021 marks the second year of the Black Unicorn Awards program and we're thrilled to share the results.

Onward and upward! **Gary S. Miliefsky, CISSP®**

Our Growing Platforms Include:

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018

INFOSEC AWARDS
CYBER DEFENSE MAGAZINE
2019

BLACK UNICORN AWARDS
2019
WINNERS

CYBER DEFENSE TV
InfoSec Knowledge is Power

CYBER DEFENSE RADIO

Dave DeWalt

Founder & CEO, NightDragon Security
Founder & Chairman, Momentum Cyber
Managing Director, Allegis Cyber

David DeWalt is a veteran CEO, advisor, and investor who has led companies, from startups to the Fortune 500, on a transformational journey of success. Focused on technology and cybersecurity, he helped create more than $20 billion of shareholder value during his 15 plus years as President and CEO of three major companies. That includes driving the most successful cybersecurity IPO ever in 2013, and leading the largest all-cash deal in technology history in 2010. Today, he serves as the CEO and founder of NightDragon Security, a dedicated cyber security investment and advisor firm. In addition, he serves as a managing director in Allegis Cyber and MomentumCyber as well as an investor and board member in the world's most innovative companies such as Delta Airlines, Five9, ForeScout, Phantom Cyber, CallSign, Claroty, Team8, DataTribe, Illusive Networks, and Optiv. He has substantial expertise in the information technology security industry and with his strategic and operational experience. Mr. DeWalt was named one of the 25 most influential executives in high technology by the readers of the industry publication CRN. He has spoken at the World Economic Forum on the issue of cyber security and keynoted at several technology industry conferences including Interop and Software 2008 and RSA.

Representative Advisory Positions & Investments

Callsign · CLAROTY · DATATRIBE · DELTA · Five9 · JASK · FORGEROCK · FORESCOUT · illusive · OPTIV · Phantom · TEAM8

Previous Experience

documentum · FIREEYE · McAfee

Robert R. Ackerman, Jr.
Founder & Managing Director
AllegisCyber Capital
Co-founder, DataTribe

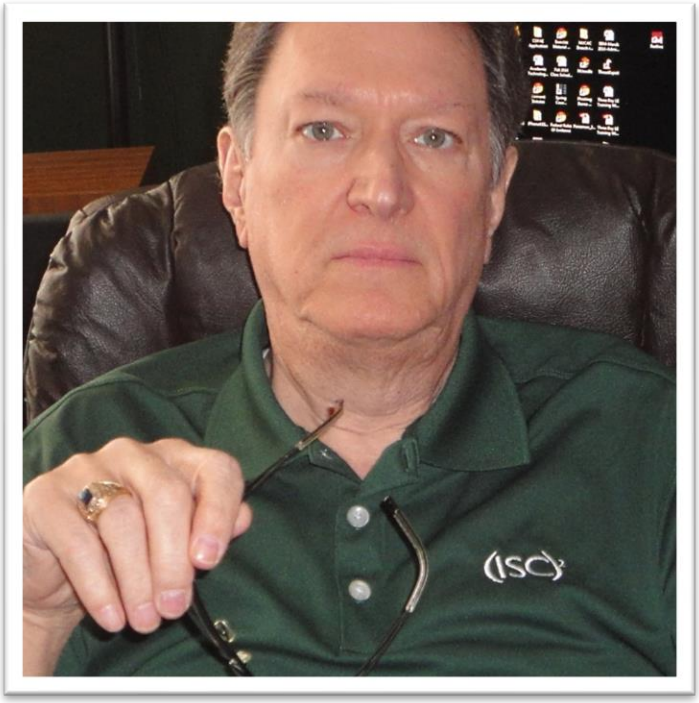
Bob Ackerman is referred to as one of “Cyber’s Money Men” by major business publications for his experience and leadership in venture capital investing in Cyber Security start-up technology companies. He has been named one of "Technology’s Top 100 Investors" by Forbes magazine and was named one of two leading cyber security investors in the world by Cyber Defense Magazine. With 20 plus years of experience as a venture capitalist, Bob is the Founder and Managing Director of Silicon Valley and Maryland-based Cyber Security venture capital firm **AllegisCyber Capital**, Co-Founder of Columbia, Maryland-based Cyber Start-up Foundry **DataTribe** and the Founder and Executive Chairman of **Founder’s Equity Partners**, a direct secondary investment firm that also invests in cyber security companies. Bob is also the Chairman of the **Global Cyber Innovation Summit**, described as the “Davos of Cyber Security”

Prior to his career as a venture capitalist, Bob was a serial entrepreneur as a CEO and founder of two successful technology companies, including leading UNIX technology company UniSoft, and InfoGear Technology Corporation, the visionary creator of the original iPhones. Bob has a degree in Computer Science and is a member of the Adjunct Faculty at the University of California’s Haas School of Business MBA program.

About AllegisCyber Capital
AllegisCyber Capital, based in Silicon Valley and Maryland, has been investing in cyber security for almost two decades in the U.S and select international markets and was the first venture firm to focus exclusively on cyber security and data science. The firm's team is replete with venture capital and start-up entrepreneurial veterans and has been described by industry press as “Cyber’s Money Men” for its domain expertise and market leadership position. Current AllegisCyber Capital investments include Area 1, Callsign, CyberGRX, Dragos, LucidWorks, SafeGuard Cyber, Shape Security, Signifyd, Source Defense, Synack and vArmour. AllegisCyber Capital partners closely with DataTribe, which grows cyber and data science technology startups in partnership with subject matter expert engineers from the U.S. intelligence community and national labs. For more information on AllegisCyber Capital, please visit www.allegiscyber.com.

About DataTribe
DataTribe was launched in 2015 with the vision of empowering cyber security and data science domain masters from the intelligence community in the Washington, D.C. region to build and grow successful startups. Founded by leading investors, startup veterans and alumni of the U.S. intelligence community, DataTribe operates as a “foundry” - commiting capital, in-kind business services and decades of professional expertise to co-build the next generation of these companies. DataTribe companies had consistently been included as Top 10 Finalists in the RSA Innovation Sandbox and in June of 2021, the World Economic Forum recognized two DataTribe companies, Dragos and ENVEIL, in its list of 100 Technology Pioneers. DataTribe is headquartered in Fulton, Maryland, the focal point for the largest concentration of advanced cyber expertise in the world. For more information, visit https://datatribe.com.

Dr. Peter Stephenson – New Black Unicorn Judge This Year!



Dr. Peter Stephenson has reactivated himself to exclusively focus on deep next generation Infosecurity product analysis for Cyber Defense Magazine after more than 50 years of active consulting and teaching. His research is in cyber-legal practice and cyber threat/intelligence analysis on large-scale computer networks such as the Internet. Dr. Stephenson was technology editor for several years for SC Magazine, for which he wrote for over 25 years. He is enabled in his research by an extensive personal research laboratory as well as a multi-alias presence in the Dark Web.

He has lectured extensively on digital investigation and security, and has written, edited or contributed to over 20 books as well as several hundred articles and peer-reviewed papers in major national and international trade, technical and scientific publications. He spent ten years as a professor at Norwich University teaching digital forensics, cyber law and information security. He retired from the university as an Associate Professor in 2015.

Dr. Stephenson obtained his PhD at Oxford Brookes University, Oxford, England where his research was in the structured investigation of digital incidents in complex computing environments. He holds a Master of Arts degree in diplomacy with a concentration in terrorism from Norwich University in Vermont.

Dr. Stephenson is a full member, ex officio board member and CISO of the Vidocq Society (http://www.vidocq.org). He is a member of the Albany, NY chapter of InfraGard. He held – but has retired from – the CCFP, CISM, FICAF and FAAFS designations as well as currently holding the CISSP (ret) designation.

He runs Cyber Defense Labs under the title Future inTense, where he does very deep dive product analysis, found here: Future inTense - Cyber Defense Magazine

Black Unicorn Winners for 2021

In this Black Unicorn Report for 2021, we've taken a few unique cybersecurity lenses to view the market and predict the future. Note that post COVID-19, the world has turned upside down and it's accelerated telecommuting and cloud-based apps (SaaS) expansion, moving us from 3-4% home workforce to over 51% and growing. Thus, the major attack vectors have shifted to the cloud and weaker home-computing hygiene. This has opened doors for increased revenues and visibility among those players who secure the cloud, SaaS apps and deal with weak, remote, exposed endpoints.

Dr. David DeWalt's Super Cycles view gives us an even clearer picture of where current and future cybersecurity investments need to be made, and therefore where we expect to find additional Black Unicorns in the coming years. According to Dr. DeWalt's NightDragon venture fund, by 2023, the cybersecurity market will be worth over $248 billion. What's driving this exponential growth?

- Attack surfaces continue to grow daily. As IT innovation around cloud, mobile, and virtualization continues, the attack surfaces that must be monitored and protected constantly grow and evolve.
- A shortage of cybersecurity workers. There's a serious shortage of professionals with real-world experience. This drives costs higher and increases demand for automation to reduce headcount.
- Regulation is increasing and evolving. To keep up with constantly changing compliance needs, organizations are increasing their focus on cybersecurity to meet regulatory requirements.
- Tactics are becoming more sophisticated: Keeping up with new tactics like monetizing attacks via cryptocurrency, renting attack infrastructure, phishing attacks, and AI require new defenses.
- The cost of cybercrime is rising fast: Cybercrime is relentlessly gaining steam across almost every industry. That's why cybercrime will cause $12 trillion in damages by 2025.

With Robert (Bob) Ackerman running one of the most innovative and successful cybersecurity venture funds in America, we have another unique investor who understands the industry including bringing a reality check and a view on what is working into the judging process and our report.

Gary Miliefsky's take on market with the PANCCD model gives us focus and helps us quickly determine where a vendor fits and how they might add value in the cyber risk reduction equation.

Dr. Stephenson's time in the trenches, teaching, testing and exploring all things cybersecurity with a keen insight into machine learning (ML), artificial intelligence (A.I.), what works and what doesn't is extremely valuable predictive intelligence on the selection of Black Unicorns.

On that note, given that we had to be pragmatic in our quest for current and future Black Unicorns, here's where we started: There are now almost 4,000 cybersecurity companies in the world. We only allowed a small number of companies based on their funding, sales growth and scalability to enter the Black Unicorn Awards contest and required they provide detailed information including funding, financials, competition and much more. In many cases this information remains confidential, at the request of the applicants.

We found some companies that didn't make the cut as Finalist for various reasons but were seriously worth a look, so we'll continue to keep an eye on them in 2022 and beyond and see how they progress. You will find all Winners and Finalists worthy of our attention and yours – you may find that they offer a unique solution missing in your cybersecurity portfolio. And here they are…

Top 10 Black Unicorns for 2021 Winners

Acronis	**www.acronis.com/en-us**
HelpSystems	**www.helpsystems.com**
Code42	**www.code42.com**
ReversingLabs	**www.reversinglabs.com**
vArmour	**www.vArmour.com**
Human Security	**www.humansecurity.com**
Attivo Networks	**www.attivonetworks.com**
Contrast Security	**www.contrastsecurity.com**
Onapsis	**www.onapsis.com**
Noname Security	**nonamesecurity.com/request-demo**

Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain-based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on-premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,600 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages.

Learn more about us and our leading cyber protection solutions at https://www.acronis.com/en-us/ and feel free to reach out to our sales team anytime!

HelpSystems

HelpSystems is a software company focused on helping exceptional organizations Build a Better IT™. Our cybersecurity and automation software simplifies critical IT processes to give our customers peace of mind. We know IT transformation is a journey, not a destination. Let's move forward. Learn more at www.helpsystems.com

Press Contact
Michael Bartley, C8 Consulting
michael@c8consulting.co.uk

Code42

Code42 is the Insider Risk Management leader. Native to the cloud, the Code42 Incydr solution rapidly detects data loss, leak and theft as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's Insider Risk solution is FedRAMP authorized and can be configured for GDPR, HIPAA, PCI and other regulatory frameworks. More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and is backed by Accel Partners, JMI Equity, NewView Capital and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020.

Learn more about us at https://www.code42.com or email information@code42.com.

ReversingLabs

ReversingLabs is the leading provider of explainable threat intelligence solutions that shed the necessary light on complex file-based threats for enterprises stretched for time and expertise. Its hybrid-cloud Titanium Platform enables digital business resiliency, protects against new modern architecture exposures, and automates manual SOC and Threat Hunting processes with a transparency that arms junior analysts to confidently take action. ReversingLabs is used by the world's most advanced security vendors and deployed across all industries searching for a more intelligent way to get at the root of the web, mobile, email, cloud, app development and supply chain threat problem, of which files and objects have become major risk contributors.

ReversingLabs Titanium Platform provides broad integration support with more than 4,000 unique file and object formats, speeds detection of malicious objects through automated static analysis, prioritizing the highest risks with actionable detail in only .005 seconds. With unmatched breadth and privacy, the platform accurately detects threats through explainable machine learning models, leveraging the largest repository of malware in the industry, containing more than 10 billion files and objects. Learn more at https://www.reversinglabs.com, or connect on LinkedIn or Twitter.

vArmour

vArmour is the leading provider of Application Relationship Management. Enterprises around the world rely on vArmour to visualize and control relationships between every user, every application, and across every environment to reduce risk and increase resiliency — all without adding new agents or infrastructure. Based in Los Altos, CA, the company was founded in 2011 and is backed by top investors including Highland Capital Partners, AllegisCyber, NightDragon, Redline Capital, Citi Ventures, SC Ventures, and Telstra. Learn more at www.vArmour.com.

Human Security

HUMAN is a cybersecurity company that protects enterprises from bot attacks to keep digital experiences human. We have the most advanced Human Verification Engine that protects applications, APIs and digital media from bot attacks, preventing losses and improving the digital experience for real humans. Today we verify the humanity of more than 10 trillion interactions per week for some of the largest companies and internet platforms. Protect your digital business with HUMAN. To Know Who's Real, visit www.humansecurity.com.

AttivoNetworks

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Data concealment technology hides critical AD objects, data, and credentials, eliminating attacker theft and misuse, particularly useful in a Zero Trust architecture. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys obfuscate the attack surface to derail attacks. Forensic data, automated attack analysis, and automation with third-party integrations serve to speed threat detection and streamline incident response. ThreatDefend capabilities tightly align to the MITRE ATT&CK Framework and deception and denial are now integral parts of NIST Special Publications and MITRE Shield active defense strategies. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com.

Contrast Security

Contrast Security is the leader in modernizing application security, embedding code analysis and attack prevention directly into software. Contrast's patented deep security instrumentation completely disrupts traditional application security approaches with integrated, comprehensive security observability that delivers highly accurate assessment and continuous protection of an entire application portfolio. This eliminates the need for expensive infrastructure workloads and specialized security experts. The Contrast Application Security Platform accelerates development cycles, improves efficiencies and cost, and enables rapid scale while protecting applications from known and unknown threats. Learn more about us at **https://www.contrastsecurity.com/** and email Jacklyn.kellick@contrastsecurity.com at anytime.

Onapsis

Onapsis protects the business-critical applications that power the global economy including ERP, CRM, PLM, HCM, SCM and BI applications from SAP®, Oracle® and leading SaaS providers. Onapsis proudly serves more than 300 of the world's leading brands including 20% of the Fortune 100 and partners with leading consulting and audit firms such as Accenture, Deloitte, IBM, PwC and Verizon. The Onapsis Research Labs is responsible for the discovery and mitigation of more than 800 zero-day business-critical application vulnerabilities.

For more information, connect with us on Twitter, LinkedIn, visit us at **https://www.onapsis.com**, or email info@onapsis.com.

Noname Security

Enterprise applications and services are only as fast and secure as the APIs that power them; however, most enterprises don't have a standardized way to inventory, monitor, and secure APIs. The growing complexity of APIs cripples' deployment velocity and APIs are quickly becoming the most frequent cyber security attack vector.

Noname Security creates the most powerful, complete, and easy-to-use API security platform that helps enterprises discover, analyze, remediate, and test all legacy and modern APIs. Noname finds and inventories all APIs; detects attacks, suspicious behavior, and misconfigurations using AI-based behavioral analysis; prevents attacks and integrates with existing remediation and security infrastructure; and actively validates APIs before deployment.

To find out how to keep your APIs out of the news, request a demo today by visiting us at https://nonamesecurity.com/request-demo

Top 10 Baby Black Unicorns for 2021 Winners

Adaptive Shield	**www.adaptive-shield.com**
Anitian	**www.Anitian.com**
Siemplify	**www.siemplify.co**
CyberProof	**www.cyberproof.com**
CYFIRMA	**www.cyfirma.com**
Nanolock Security	**www.nanolocksecurity.com**
Red Piranha	**www.redpiranha.net**
ThreatLocker	**www.threatlocker.com**
Valtix	**www.valtix.com**
XM Cyber	**www.xmcyber.com**

Adaptive Shield

Adaptive Shield, the leading SaaS Security Posture Management (SSPM) company, enables security teams to see and fix configuration weaknesses quickly in their SaaS environment, ensuring compliance with company and industry standards. Adaptive Shield works with many Fortune 500 enterprises to help them gain control over their SaaS threat landscape. Our management team has vast experience in cybersecurity leadership, delivering cybersecurity solutions and cloud enterprise software. For more information, visit us at **www.adaptive-shield.com** or follow us on LinkedIn.

Learn how you can secure your company's SaaS security now.

Anitian

Anitian delivers the fastest path to application security and compliance in the cloud. Anitian's Compliance Automation Platform and SecureCloud DevSecOps Platform help high-growth companies get their SaaS applications to the cloud and market quickly, so they can unlock revenue in weeks, not months or years. Our automated cloud application security platforms deliver a full suite of security controls – both pre-engineered and pre-configured to meet rigorous security standards such as FedRAMP, CMMC, DoD SRG, and PCI. Anitian's pre-built environment and platforms use the full power and scale of the cloud to accelerate time-to-production, time-to-market, and time-to-revenue so you can start secure, start compliant, and stay ahead. Learn more at http://www.anitian.com or follow Anitian on LinkedIn or Twitter.

Siemplify

Siemplify is a SOAR solution which stands for Security Orchestration, Automation, and Response. It enables case management and the running of Playbooks on incoming alerts, with the goal of reducing the amount of time an analyst must spend on repetitive tasks which can be easily automated.

Siemplify is on a mission to reimagine security operations. That tirelessly pursue simplicity and a stellar user experience – think Salesforce but for security operations professionals – to help SOC practitioners move beyond the daily grind so they can concentrate on what matters most: investigating and remediating real threats, fast.

Siemplify embeds security know-how into the platform, relieving the heavy load and expectation placed on the analyst to be an expert in all things security.

Visit us at https://www.siemplify.co/.

CyberProof

CyberProof is a security services company that intelligently manages your organization's incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact. CyberProof is part of the UST family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services. If you want to speak to one of our cyber experts email us at info@cyberproof.com or visit our website: **www.cyberproof.com**

CYFIRMA

CYFIRMA is a threat discovery and cyber-intelligence company with the world's first platform that can deliver predictive cyber-intelligence.

The company's flagship product, DeCYFIR, arms governments and businesses with personalized intelligence where insights are tailored to their industry, geography and technology. DeCYFIR provides clients with multi-layered intelligence covering strategic, management and operational insights. DeCYFIR's ability to combined cyber-intelligence with attack surface discovery, vulnerability intelligence, brand intelligence, situational awareness and digital risk protection sets it apart from the competition. The platform provides risk and hackability scores to help clients prioritize security actions. Clients also receive insights that will enable them to conduct effective intelligence hunting and attribution, connecting the dots between hacker, motive, campaign and method to gain a comprehensive view of their threat landscape.

With DeCYFIR, clients receive early warnings of impending cyberattacks so they can act quickly to avoid a breach. DeCYFIR is designed to meet the stringent demands of CISOs, CROs, and Security Operations teams.

The company is also behind the cutting-edge digital risk protection platform, DeTCT. DeTCT helps clients uncover their attack surfaces, know their vulnerabilities, quickly gain awareness of any data breach or leak. DeTCT also helps clients protect their brand and reputation by unraveling any copyright infringement and executive impersonation.

CYFIRMA is headquartered in Singapore with offices in Japan, India, and the US. The company is funded by Goldman Sachs, Zodius Capital, and Z3 Partners. Current reference clients include Mitsubishi Corporation, TOSHIBA, NEC, Suntory System Technology, SBI BITS, Zuellig Pharma and NTT Data Intellilink.

Learn more about CYFIRMA here: cyfirma.com

Nanolock Security

NanoLock Security's zero-t
rust, device-level protection and management secure IoT, OT and connected devices against persistent cyberattacks by outsiders, insiders and supply chain adversaries, including billions of devices that other technologies cannot protect. Our lifetime protection and management solution takes zero-trust to the device-level with an ironclad protection, secured and managed firmware updates, reliable status and alerts and unique forensic data. NanoLock fuels the IoT and IIoT revolution with an enduring and affordable zero-trust protection that is mandatory to critical infrastructures, such as industrial companies and utilities that are looking to ensure the integrity of their devices, maintain business continuity and protect revenues. NanoLock secures connected devices like smart meters, industrial machines, smart lighting, gateways, data concentrators, and many more, against a wide range of persistent attacks, including ransomware, fraud, theft, DDoS and others. NanoLock is working with major utilities, industrial companies and large ecosystem partners in Japan, Italy, Spain, Switzerland, Netherlands, India, Singapore, US and Israel. NanoLock's team of cybersecurity veterans combines business strategy and cyber security expertise. NanoLock is headquartered in Israel with offices in the US, Europe and Japan.
Visit **www.nanolocksecurity.com** for more information and follow NanoLock on Twitter and LinkedIn.

Red Piranha

Red Piranha is an Australian-based manufacturer of advanced cybersecurity ecosystem solutions and services for government and defence organisations. An ISO 27001:2013, multi-award-winning organisation, we are committed to deploying solutions for all sizes in dealing with cyber-attacks and the evolving threat landscape. Red Piranha's Crystal Eye XDR as a 100% Australian IP owned, managed and manufactured operation enables Australia to join an exclusive set of nations: the United States, China and Israel, who can export the Crystal Eye XDR level of cybersecurity technology in turn, providing Australia with true sovereign level data integrity and cybersecurity.

To learn more about Red Piranha's Crystal Eye XDR and our extensive range of cybersecurity solutions, please visit **https://redpiranha.net**

ThreatLocker

ThreatLocker® is a global cybersecurity leader, providing enterprise-level cybersecurity tools to improve the security of servers and endpoints. ThreatLocker's combined Application Whitelisting, Ringfencing™, Storage Control and Privileged Access Management solutions are leading the cybersecurity market towards a more secure approach of blocking all unknown application vulnerabilities. To learn more about ThreatLocker

visit: www.threatlocker.com
Visit www.threatlocker.com to learn more.

Valtix

Valtix is on a mission to enable organizations with security at the speed of the cloud. The first multi-cloud network security platform delivered as a service, Valtix was built to combine robust security with cloud-first simplicity and on-demand scale. Powered by a cloud-native architecture, Valtix provides an innovative approach to cloud network security that is 1000x faster to adapt to new apps or changes than virtual firewalls. The result: security that is more effective and aligned to cloud agility requirements. With Valtix, organizations don't have to compromise in the cloud. They can meet critical security and compliance requirements without inhibiting the speed of the business.

Get started with a free trial and a cloud visibility report at http://www.valtix.com

XM Cyber

XM Cyber is the global leader in attack path management. XM Cyber brings a new approach that uses the attacker's perspective to find and remediate critical attack paths across on-premises and multi-cloud networks. The XM Cyber platform enables companies to rapidly respond to cyber risks affecting their business-sensitive systems by continuously finding new exposures, including exploitable vulnerabilities and credentials, misconfigurations, and user activities. XM Cyber constantly simulates and prioritizes attack paths putting mission-critical systems at risk, providing context-sensitive remediation options. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel. Learn more about us at **www.xmcyber.com** and email info@xmcyber.com anytime.

Top 10 Cybersecurity Startups for 2021 Winners

build.security	www.console.build.security
Cervello	www.cervellosec.com
Confluera	www.confluera.com
CrowdSec	www.crowdsec.net/
Defendify	www.defendify.io/
Don't Be Breached	www.dontbebreached.com
Hyperproof	www.hyperproof.io/
Keyavi Data Corp.	www.keyavi.com/our-technology/
Stellar Cyber, Inc.	www.stellarcyber.ai/
Strata Identity	www.strata.io/

Build.security

Build.security makes it easy to build and manage secure authorization policies across all of your applications and services. Leveraging Open Policy Agent (OPA), we make it easy for developers to centrally manage policies in highly distributed environments, and eliminate the common headaches of managing access control.

Get started with a free account by going to build.security/go or send us an email to hell@build.security to tell us about what you're building.

Learn more about us @ **https://console.build.security/.**

Cervello

Cervello is a rail cybersecurity leader dedicated to protecting the quality of railway safety, reliability and availability worldwide. Cervello offers the first and only security platform that blends patented Zero-Trust Signalling Authentication technology, nation-state grade threat intelligence and actionable response capabilities, enabling rail organizations to perform with full visibility and control of their operational assets, infrastructure activity and safety / mission-critical procedures.

Contact us for more information at info@cervellosec.com or visit our website at **https://www.cervellosec.com.**

Confluera

Confluera is the leading provider of Cloud eXtended Detection and Response (CxDR). Recognized by Forbes as one of the Top 20 Cybersecurity Startups to Watch in 2021, Confluera is the only vendor that offers real-time sequencing of various attack steps found in modern cyberattacks. Confluera's patented machine-learning technology avoids the traditional error-prone, manual, and time-consuming task of alert correlation. Instead, it stitches together only the alerts that are accurately determined to be associated with the cyberattack. The resulting real-time threat storyboard applies to multiple environments including cloud containers and Kubernetes. With Confluera, organizations can avoid breaches by reducing the cyberattack detection and response time from months to days. To learn more about Confluera's award-winning solution, visit **www.confluera.com**

CrowdSec

CrowdSec is an open-source security engine able to analyze user behavior & provide an adapted response to all kinds of attacks. What's more, each time an IP is blocked, users in the community are informed. Therefore, CrowdSec combines both behavior and reputation, forming a global cyber defense shield. Already used in 100+ countries, CrowdSec builds a real-time IP reputation database that will benefit individuals, companies, and institutions.
We leverage the crowd power to make the Internet safer, together.

Learn more about us at **https://crowdsec.net/** and https://github.com/crowdsecurity/crowdsec

Defendify

Defendify is pioneering cybersecurity for organizations without security teams, including IT and technology providers.

Delivering multiple layers of protection, Defendify provides cybersecurity expertise, support, and its all-in-one, easy-to-use platform designed to continuously strengthen cybersecurity across people, process, and technology.

Defendify streamlines cybersecurity assessments, testing, policies, training, detection, and response in one consolidated and cost-effective cybersecurity solution.

Learn more about us at [Defendify.com]Defendify.com or book a demo today to see our all-in-one cybersecurity platform.

Don't Be Breached

The **Database Cyber Security Guard** product is a **Don't Be Breached** company product. It protects credit card, tax ID, medical, social media, corporate, manufacturing, law enforcement, defense, homeland security and public utility data in DB2, Informix, MariaDB, MySQL, Oracle, PostgeSQL, SQL Server and SAP Sybase databases. The product performs a **Deep Packet Inspection** and **Analysis** to learn what the normal database SQL activity is. Database servers servicing 500 to 10,000 end-users 24x7 typically process daily 2,000 to 10,000 unique query or SQL commands that run millions of times a day. This SQL activity is very predictable. An **Advanced SQL Behavioral Analysis** of the network packets allows abnormal database activity by **Hackers, Rogue Insiders** and **Third Party Cyber Risks** to be detected and shut down immediately. Advanced SQL Behavioral Analysis of the packet flow allows never before observed SQL queries, never before observed IP addresses and non-normal amounts of confidential database data being transmitted to be detected within a few milli-seconds. The product runs silently on a network tap or proxy server. Does not need to connect to the monitored databases. Has a low overhead and disk space usage.

Learn more about us at https://dontbebreached.com or email sales@dontbebreached.com.

Hyperproof

Hyperproof is a cloud-based compliance operations software that's specifically built to manage compliance activities and risks day in and day out. The platform supports any cybersecurity, data privacy, and risk management frameworks a company wants to adhere to, and helps users identify and map the common controls that can satisfy multiple frameworks. Hyperproof provides a highly efficient system for managing evidence centrally, allowing evidence to be easily reused for multiple audits and across business units/product groups. Organizations can save a tremendous amount of time by using Hyperproof's built-in tools to automate evidence collection, control monitoring, and project management chores. The software not only reduces administrative work from compliance processes, but also helps organizations mitigate their risks on an ongoing basis—giving them the critical oversight they need in a time when the regulatory and economic environments are uncertain and cybersecurity risk is on the rise.

Visit hyperproof.io to learn how Hyperproof can help you gain the visibility, efficiency, and consistency you need to stay on top of all your security assurance and compliance work.

Keyavi Data Corp.

Headquartered in Denver, Keyavi's award-winning self-protecting, intelligent and self-aware cybersecurity technology enables an individual piece of data to think for itself, secure itself, refuse access to unauthorized users, stay continually aware of its surroundings and automatically report back to its owner. The company's API platform and a full suite of applications riding on that platform also provide data owners with powerful controls to allow, revoke or deny access to their information – no matter who has it, where it's stored, or how many copies exist. Under development for years before launching in 2020, this multi-patented technology is so unique and innovative that leading industry analyst firm Omdia designated "self-protecting data solutions" as a new cybersecurity industry category. Keyavi's easy-to-use yet robust solution delivers the ultimate in peace of mind for public and private organizations, their remote workforces and partner ecosystems in solving the security challenges of controlling confidential and intellectual property from data leaks, breaches and ransomware.

To learn more about Keyavi and its breakthrough technology, visit https://keyavi.com/our-technology/. Follow Keyavi on LinkedIn, Facebook, YouTube and Twitter.

Stellar Cyber, Inc.

Stellar Cyber's Open XDR platform delivers Everything Detection and Response by ingesting data from all tools, correlating incidents across the entire attack surface, delivering high-fidelity detections, and responding to threats automatically through AI and machine learning. Our XDR Kill Chain™, fully compatible MITRE ATT&CK framework, is designed to characterize every aspect of modern attacks while remaining intuitive to understand. This reduces enterprise risk through early and precise identification and remediation of all attack activities while slashing costs, retaining investments in existing tools and accelerating analyst productivity. Typically, our platform delivers a 20X improvement in MTTD and an 8X improvement in MTTR.

Learn more about us at https://stellarcyber.ai/ and email info@stellarcyber.ai anytime.

Strata Identity

Strata is pioneering the concept of identity orchestration for distributed, multi-cloud identity. The Maverics Platform enables enterprises to seamlessly unify on-premises and cloud-based authentication and access systems for consistent identity management in multi-cloud environments. Strata's distributed approach to identity enables organizations to break decades-old vendor lock-in, preventing a broader transition of enterprise workloads to the public cloud. The company's founders co-authored the SAML open standard for identity interoperability, created the first cloud identity services, delivered the first open-source identity products, and are now building the first distributed identity platform. For more information, visit us on the Web and follow us on LinkedIn and Twitter.

Top 10 MSSPs for 2021 Winners

Herjavec Group	www.herjavecgroup.com/
Simeio	www.simeio.com/
Konica Minolta	www.konicaminolta.eu/eu-en
AT&T Cybersecurity	www.att.com/
NTT Ltd.	www.hello.global.ntt
Trustwave	www.trustwave.com
Orange Cyberdefense	www.orangecyberdefense.com/
Accenture	www.accenture.com
IBM Managed Security Services	www.ibm.com
Secureworks	www.secureworks.com/

Herjavec Group

Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. HG has been recognized as one of the world's most innovative cybersecurity operations leaders, and excels in complex, multi-technology environments. We have expertise in comprehensive security services, including Advisory Services, Technology Architecture & Implementation, Identity & Access Management, Managed Security Services, Threat Hunting & Management, Digital Forensics and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, Canada and India. For more information, visit HerjavecGroup.com or contact a security specialist at: info@herjavecgroup.com.

Simeio

Simeio provides the industry's most complete Identity and Access Management solution delivered as a service and interoperable with leading IAM tools. We protect over 150 million identities globally for enterprises, institutions, and government entities of all sizes. Our platform and services provide the following set of enterprise-grade security and identity capabilities: Access Management and Federation, Access Request, Directory Services, Identity Governance and Administration, Identity Management and Administration, Privileged Access Management, Security & Risk Intelligence, Data Security & Loss Prevention, and Cloud Security. Simeio IDaaS—which consists of Simeio Identity Orchestrator™ (IO), Simeio Identity Intelligence Center™ (IIC), and managed identity services—brings together best-in-class processes, professionals, and technologies focused entirely on management and protection of identities and related access controls. Headquartered in Atlanta, Georgia, and with Security Operations Centers worldwide, Simeio provides services to Global 2000 companies across all industries, and government entities. For more information, please visit **http://www.simeio.com/**.

Konica Minolta

All Covered, a division of Konica Minolta Business Solutions, U.S.A., Inc., is a leading nationwide IT Services company that helps businesses achieve their goals through better management of information and more effective collaboration. Our commitment to innovation in providing industry-leading solutions has been repeatedly recognized by some of the IT industry's most respected publications and organizations, including CRN's SP 500 and Channel Future's MSP 501. We have also been acknowledged for our expertise across vertical markets such as education, finance, healthcare and legal. Our IT engineers are well versed in the nuances and regulations of each market segment. From network design to helpdesk support, IT security, cloud services and managed IT, All Covered customizes solutions to its clients' business and application needs. Visit us online and follow All Covered on Facebook, YouTube, Linked In and Twitter.

AT&T Cybersecurity

AT&T* is delivering a new, global managed Secure Access Service Edge (SASE) offering. AT&T SASE with Palo Alto Networks is an integrated solution that brings together software-defined wide area networking (SD-WAN) technology, security capabilities and fiber-based network connectivity. The comprehensive solution, with expertise in design configuration, deployment, and 24/7 management from a single provider, helps enterprises and state and local governments to modernize their networks, provide robust security, and improve user experience and visibility.

AT&T Business combines leading managed SD-WAN services, cybersecurity capabilities, and the power of 5G to deliver cutting

We help family, friends and neighbors connect in meaningful ways every day. From the first phone call 140+ years ago to mobile video streaming, we @ATT innovate to improve lives.

AT&T Communications is part of AT&T Inc. (NYSE:T). For more information, please visit us at att.com.

NTT Ltd.

NTT Ltd. is a leading global technology services company. Working with organizations around the world, we achieve business outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital and secure. Our global assets and integrated ICT stack capabilities provide unique offerings in cloud-enabling networking, hybrid cloud, data centers, digital transformation, client experience, workplace and cybersecurity. As a global ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace that spans 57 countries, trading in 73 countries and delivering services in over 200 countries and regions. Together we enable the connected future.

Visit us at hello.global.ntt.

Trustwave

Trustwave is a leading cybersecurity and managed security services provider focused on threat detection and response. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely.

For more information about Trustwave, visit **https://www.trustwave.com**

Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.
We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.
Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.
Twitter: @OrangeCyberDef
Media Contact
Babel PR for Orange Cyberdefense
orangecyberdefense@babelpr.com

Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 569,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

IBM Managed Security Services

IBM is a leading global hybrid cloud and AI, and business services provider, helping clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. Nearly 3,000 government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently, and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and business services deliver open and flexible options to our clients. All of this is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity, and service.
For more information, visit www.ibm.com

Secureworks

Secureworks is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions. The company launched Secureworks Taegis™ XDR (Extended Detection and Response) a cloud-native SaaS solution that combines Secureworks' security operations expertise and threat intelligence capabilities to detect and respond to attacks across cloud, endpoint, and network environments. It covers more than 90% of tactics, techniques, and procedures (TTPs) across all categories of the MITRE framework and provides a comprehensive view of environments through 40+ third-party integrations. Check it out for yourself using the new interactive and publicly available Taegis XDR Adversary Software Coverage (ASC) Tool, which maps over 500 unique adversarial software types against the MITRE ATT&CK framework.

To learn more visit Secureworks.com. Connect with Secureworks via Twitter, LinkedIn and Facebook. Whether you're a customer or a prospect, contact us anytime.

Top 10 Cybersecurity Experts for 2021 Winners

Shay Levi	**Noname Security**
Mario Vuksan	**ReversingLabs**
Jeffrey Carpenter	**Secureworks**
Aleksandr Yampolskiy	**SecurityScorecard**
Craig Young	**Tripwire Inc.**
Kaarel Kotkas	**Veriff**
Robert Herjavec	**Herjavec Group**
Joe Slowik	**Gigamon**
Elliot Lewis	**Keyavi Data Corp.**
Zubair Ansari	**CionSystems**

Top 10 Women in Cybersecurity for 2021 Winners

Angela Schoeman	**CyberProof**
Camellia Chan	**Flexxon Pte Ltd**
Carolyn Crandall	**Attivo Networks**
Corinna Krueger	**SafeBreach**
Jadee Hanson	**Code42**
Jocelyn King	**Keyavi Data Corp.**
Kate Kuehn	**vArmour**
Michelle Welch	**WatchGuard Technologies**
Netta Schmeidler	**Morphisec**
Saryu Nayyar	**Gurucul**

Top 10 Chief Information Security Officers (CISOs) for 2021 Winners

Jadee Hanson	**Code42**
Ryan Weeks	**Datto**
Sounil Yu	**JupiterOne**
T.J. Minichillo	**Keyavi Data Corp.**
Jairo Orea	**Kimberly-Clark**
Ken Deitz	**Secureworks**
Terence Jackson CISM, CDPSE, GRCP	**Thycotic**
Paul (Kip) James	**TTEC**
Sunil Seshadri	**Visa**
Alberto Mischi	**Amazon.com**

Finalists for Top 10 Black Unicorns 2021

Avanan	www.avanan.com
Cynet	www.cynet.com
Flexxon	www.flexxon.com
Fluency	www.fluencysecurity.com
Morphisec	www.morphisec.com
Pentera	www.pentera.io
Resecurity	www.resecurity.com
SaasPass	www.saaspass.com
SecuritySecorecard	www.securityscorecard.com
ThreatBook	www.threatbook.cn
Versa Networks	www.versa-networks.com

Avanan

Avanan's AI protects cloud email and collaboration suites from cyber attacks that evade default and advanced security tools. Its invisible, multi-layer security enables full-suite protection for cloud collaboration solutions such as Office 365, G-Suite, Teams, and Slack. The platform deploys in one click via API to prevent Business Email Compromise and block phishing, malware, data leakage, account takeover and shadow IT across the enterprise. Avanan replaces the need for multiple tools to secure the entire cloud collaboration suite, with a patented solution that goes far beyond any other Cloud Email Security Supplement.

You can learn more about us at www.Avanan.com or email info@avanan.com

Cynet

Cynet enables any organization to simplify their cybersecurity, streamlining and automating their entire security operations while providing enhanced levels of visibility and protection across endpoints, users, networks and SaaS applications, regardless of the security team's size, skill or resources and without the need for a multi-product security stack. It does so by natively consolidating the essential security technologies needed to provide organizations with comprehensive threat protection into a single, easy-to-use XDR platform; automating the manual process of investigation and remediation across the environment; and providing a 24-7 proactive MDR service - monitoring, investigation, on-demand analysis, incident response and threat hunting - at no additional cost.

Closing call to action: Learn more about Cynet: https://www.cynet.com

Flexxon

Flexxon is the leading brand to design, manufacture, and retail industrial NAND flash storage and memory devices. Our key emphasis is to provide top-notch memory solutions ensuring the highest level of data security. We have a range of versatile compact memory storage solutions to serve every sector; specifically the CYBERSECURITY, INDUSTRIAL, MEDICAL & AUTOMOTIVE (CIMA) applications.

Our knowledge and expertise in NAND technology spurred us to develop new cybersecurity solutions, including our latest innovation, X-PHY® AI embedded cyber-secure SSD which has cybersecurity capabilities embedded at the firmware level. This world's first cybersecurity solution certifies as the last layer of defense against cyber threats and won the Cyber Security Agency of Singapore Award. With a vision to revolutionise technologies for good, Flexxon remains at the forefront of innovation and is dedicated to maintaining Data Integrity, Data Confidentiality, and Cybersecurity intact for individuals and organisations around the world.

Learn more about us at https://www.flexxon.com or get in touch with us at flexxon@flexxon.com.

Fluency

Fluency is a pioneer in Security Automation and Orchestration (SAO). Fluency's approach to SAO is unique in that it is data centric, providing a central log management to empower the decision-making process that is SAO. Offering the industry's fastest big data solution, Fluency empowers organizations to cost effectively, yet powerfully, harness Machine Learning (ML) and Artificial Intelligence (AI). Fluency's patent-pending technology combines AI and ML to arm companies with powerful response orchestration – resulting in a smarter, continually-improving view of the network and host data as well as alerts from traditional security devices.

To learn more, visit the website; https://www.fluencysecurity.com/

Morphisec

Morphisec is the world leader in providing advanced security solutions for midsize to small enterprises around the globe. We simplify security and can automatically block modern attacks from the endpoint to the cloud. Unlike traditional security solutions relying on human intervention, our solutions deliver operationally simple, proactive prevention. We protect businesses around the globe with limited security resources and training from the most dangerous and sophisticated cyber attacks.

Learn more about us: https://www.morphisec.com/
Meet us at Black Hat USA 2022: https://engage.morphisec.com/meet-morphisec-at-upcoming-events
Email us: ryan.edwards@morphisec.com

Pentera

Pentera (formerly Pcysys) was founded by Arik Liberzon in 2015 and is headquartered in Petach Tikva, Israel, with locations in Boston, United States, London, United Kingdom and Hamburg, Germany. Liberzon previously led the Cyber Warfare group in the Israeli Defence Force's Computer Service Directorate, a group responsible for penetration testing of strategic asset networks and national mission-critical systems. Over 300 organizations across more than 30 countries around the globe rely on Pentera to discover their actual security exposure in real time.

Pentera has the only technology capable of modeling attacker behaviors in a complete and autonomous way. The company removes the need for manual penetration testing and red teaming through its unique technology that adapts its attack path with every new finding and compromise using its arsenal of proprietary tactics, techniques and procedures. Pentera's agentless architecture mimics the operation of an advanced attacker without a trace or requiring any prior network knowledge, stress testing, or existing detection and response technologies.

To learn more about us please visit; https://www.pentera.io/

Resecurity

Founded in 2016, Resecurity, Inc. has been globally recognized as one of the world's most innovative cybersecurity companies with the sole mission of protecting enterprises globally from evolving cyber threats through intelligence. Resecurity, Inc. has developed a global reputation for providing best of breed data-driven intelligence solutions.

Learn more about us at https://www.resecurity.com and email sales@resecurity.com anytime.

SaasPass

SAASPASS is the innovative disruptive Identity & Access Management platform built on a Passwordless architecture and Zero Trust Security model.

The next-generation IAM solution includes: multi-factor authentication, single sign-on, enterprise password manager, shared access manager, universal directory, privileged access management, access control policies, adaptive authentication, endpoint protection, MFA API and passwordless security. SAASPASS has over 100 thousand pre-built multi-factor authentication integrations ranging from modern apps like Google Workspace, Box, Microsoft Office 365 to legacy protocols like Microsoft Exchange ActiveSync and MAPI. SAASPASS has over 100 thousand pre-built apps for the single sign-on. In addition, SAASPASS supports over 15 multi-factor authentication methods including passwordless MFA and FIDO. You can sync multiple external directories like AD with the SAASPASS universal directory or just SAASPASS as a directory. SAASPASS is available as a cloud offering and on-premise.

Learn more about why companies are choosing us at https://saaspass.com/ and email sales@saaspass.com anytime.

SecuritySecorecard

Funded by world-class investors including Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 10 million companies continuously rated. Founded in 2013 by security and risk experts, Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 16,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, and cyber insurance underwriting. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees, and vendors. Every company has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

ThreatBook

ThreatBook is China's first security threat intelligence company, dedicated to providing real-time, accurate and actionable threat intelligence to block, detect and prevent attacks. The ThreatBook team has in-depth understanding of China's distinct cyber security landscape as well as an international perspective of the global cyber security space. ThreatBook offers a variety of SaaS-based threat intelligence products and services world widely, helps partners and customers to improve their existing detection and defense capabilities at different stage of threat attack, and enables industry customers to deal with complex, continually changing threats in a fast, accurate and cost-effective manner.

Versa Networks

Versa Networks, the leader in SASE, combines extensive security, advanced networking, industry leading SD-WAN, genuine multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and Service Providers, and via the simplified Versa Titan cloud service designed for Lean IT. Thousands of customers globally with hundreds of thousands of sites trust Versa with their networks, security, and clouds. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, Liberty Global Ventures, Princeville Capital, RPS Ventures and Triangle Peak Partners. For more information, visit https://www.versa-networks.com or follow Versa Networks on Twitter @versanetworks.

Finalists for Top 10 Baby Black Unicorns 2021

Blue Hexagon	**www.bluehexagon.ai.**
Cyvatar	**www.cyvatar.ai**
Dasera	**www.dasera.com**
DNSFilter	**www.DNSFilter.com**
Eclypsium	**www.eclypsium.com**
Ermetic	**www.ermetic.com**
InQuest	**www.inquest.net**
JupiterOne	**www.JupiterOne.com**
Kasada	**www.kasada.io**
TrueFort	**www.truefort.com**
TruU	**www.truu.ai.**

Blue Hexagon

Founded in 2017, Blue Hexagon is a deep learning innovator of Cyber AI You Can Trust™ to stop cyber adversaries and malware at sub-second speed. Blue Hexagon Agentless Cloud-Native AI Security deploys within minutes and delivers actionable visibility, real-time threat defense, and continuous compliance across all cloud workloads, network, and storage, at runtime. The agentless solution does not impact performance or data privacy and confidentiality, eliminates Security-DevOps friction and supply-chain risk, and supports all workload types and OS platforms across major cloud providers - reducing enterprise security overhead and cost while significantly improving their cloud security posture and visibility.

Blue Hexagon is headquartered in Sunnyvale, CA, and is backed by Benchmark and Altimeter Capital. Follow us on Twitter @bluehexagonai or on the Web at www.bluehexagon.ai.

Learn more about us at https://bluehexagon.ai or try and buy here https://bluehexagon.ai/cloud-security-free-trial-lp/ or on AWS Marketplace. You can also email us at inquiries@bluehexagon.ai

Cyvatar

Cyvatar is committed to making cybersecurity effortless for everyone. As the industry's first membership-based, cybersecurity-as-a-service (CSaaS) company, it's our mission to transform the way the security industry builds, sells, and supports cyber solutions. We empower our members to achieve successful outcomes by providing expert advisors, proven technologies, and a strategic process roadmap to guarantee results that map to their business drivers. Our approach is rooted in proprietary ICARM (installation, configuration, assessment, remediation, maintenance) methodology that delivers smarter, measurable security solutions for superior compliance and cyber-attack protection faster and more efficiently, all at a fixed monthly price. And because we're a subscription, members can cancel anytime. Cyvatar is headquartered in Irvine, California with a design hub in Austin and other locations around the world. Begin your journey to security confidence at https://cyvatar.ai/ and follow us on LinkedIn and Twitter.

Dasera

Dasera helps cloud-first organizations secure data that traditional tools like access control and DLP aren't designed to address. The platform manages data sprawl, monitors data in-use, and discovers misconfiguration and permission errors. Only Dasera secures the entire data lifecycle — from creation to archival — to cripple breaches once and for all. The platform finds where sensitive cloud data is stored, detects data store misconfigurations, analyzes permissions, monitors data in use, and tracks data lineage. Recognized among the Top 10 cloud security startups in 2021 by CRN, Dasera was co-founded by serial-entrepreneurs Ani Chaudhuri and Noah Johnson and is backed by Sierra Ventures.

Learn more about us at https://www.dasera.com and email sales@dasera.com anytime.
.

DNSFilter

Founded in 2015, DNSFilter provides security via DNS that protects over 15,000 organizations and 4M end users from online security threats and undesirable content using artificial intelligence—all while running on the fastest and most reliable network within the DNS security industry. DNSFilter catches threats up to 154 hours faster than competitors, and uniquely identifies more than 76% of domain based threats including zero day threats.
To find out how to protect your edge network, visit www.DNSFilter.com.

Eclypsium

Eclypsium is the enterprise firmware security company. Our comprehensive, cloud-based platform identifies, verifies and fortifies firmware and hardware wherever it exists in your extended global networks: in laptops, tablets, servers, network gear and connected devices. The Eclypsium platform secures against persistent and stealthy firmware attacks, provides continuous device integrity, delivers firmware patching at scale, and prevents ransomware and malicious implants. Serving security -conscious Fortune 1000 enterprises and federal agencies, Eclypsium was named a Gartner Cool Vendor in Security Operations and Threat Intelligence, a TAG Cyber Distinguished Vendor, one of the World's 10 Most Innovative Security Companies by Fast Company.
To learn more about how Eclypsium can protect your organization, visit eclypsium.com or email info@eclypsium.com.

Ermetic

Ermetic helps prevent breaches by reducing the attack surface of cloud infrastructure and enforcing least privilege at scale in the most complex environments. The Ermetic SaaS platform is an identity-first security solution that provides holistic, multi-cloud protection using advanced analytics to continuously analyze and remediate risks associated with permissions, configurations and behavior across the full cloud infrastructure stack.The company is led by proven technology entrepreneurs whose previous companies have been acquired by Microsoft, Palo Alto Networks and others. Ermetic has received funding from Accel, Glilot Capital Partners, Norwest Venture Partners and Target Global. To learn more visit https://ermetic.com/ and follow us on LinkedIn, Twitter and Facebook. For a product demo see https://l.ermetic.com/get-a-demo or write to us at info@ermetic.com.

InQuest

InQuest is a cybersecurity services and solutions company founded in 2013 by a well-versed team hailing from both the public and private sectors. Our platform is purpose-built by SOC analysts for SOC analysts and network defenders, with cloud and on-premises capabilities in threat prevention, breach detection, threat hunting and data leakage discovery. We've automated much of the typically mundane tasks of the SOC analyst, including fully integrating with Joe Sandbox, resulting in analyst level scrutiny of data-in-motion at carrier class speeds as well as data-at-rest, all the while reducing frustration, and in-turn, allowing precious human time to be spent where it matters. For more information, visit https://inquest.net.

JupiterOne

JupiterOne is a knowledge base for all of your cyber assets and relationships, a platform for security engineering and automation, a virtual assistant to the security operations team, and a lightweight system to achieve continuous compliance as code.

JupiterOne's platform enables security teams to take command of their entire digital environment and cyber assets base. Know more, and fear less with JupiterOne.

To learn more and set up a free account, visit JupiterOne.com and get started with JupiterOne today.

Learn more about JupiterOne

- JupiterOne Lands $19 Million Funding Round to Fuel Data-Driven Approach to Cyber Asset Management
- See JupiterOne at an upcoming virtual conference
- Social media: Twitter | LinkedIn | YouTube

Kasada

Kasada is the most effective and easiest way to defend against advanced persistent bot attacks across web, mobile, and API channels. With Kasada, trust in the Internet is restored by foiling even the stealthiest cyber threats, from credential abuse to data scraping. The solution invisibly stops automated threats while inflicting financial damage to attackers, destroying their ROI. With the ability to onboard in minutes, Kasada ensures immediate and long-lasting protection while empowering enterprises with optimal online activity. Kasada is based in New York and Sydney, with offices in Melbourne, San Francisco, and London. For more information, please visit www.kasada.io and email us at enquiries@kasada.io.

TrueFort

TrueFort is the leader in delivering zero trust protection for critical applications. Leveraging unique real-time, adaptive trust, and cloud-to-ground capabilities, TrueFort's Fortress platform detects and contains security threats before they become business risks. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unprecedented application visibility and security. To learn more, visit https://truefort.com or email sales@truefort.com.

TruU

TruU enables enterprises to eliminate passwords and badges to truly revolutionize the way workforces experience their workplace. We offer unique passwordless identity through adaptive MFA built on biometrics and behavioral identity that unifies access to physical and digital resources across the enterprise. More information can be found at www.truu.ai. Join the conversation on LinkedIn.

Finalists for Top 10 Cybersecurity Startups 2021

Axiado Corporation	**www.axiado.com**
Britive	**www.britive.com**
Reflectiz	**www.reflectiz.com**
Enso Security	**www.enso.security**
Grip Security	**www.grip.security**
Qrypt, Inc.	**www.qrypt.com**
Rezilion	**www.rezilion.com**
Sepio Systems	**www.sepio.systems**
Cythereal	**www.cythereal.com**
uQontrol	**uQontrol.com**
Satori	**www.satoricyber.com**

Axiado Corporation

Axiado is a security processor company founded in San Jose, California, in 2017. The company is redefining hardware root of trust with hardware-based security technologies, including per-system AI. Its Secure Vault™ boot system, Secure AI™ engine, secure memory controllers and unique key management units protect sensitive data from the attack vulnerabilities found in current processors, and ensure security for every system.

Find out more about Axiado at https://axiado.com or contact us at info@axiado.com.

Britive

The Britive Cloud Privilege Management Platform is a cloud-native, 100% API based, security solution built for the most demanding cloud-forward enterprises. It empowers teams across cloud infrastructure, DevOps, and security functions with dynamic and intelligent privileged access administration solutions for multi-cloud environments.

The Britive platform helps organizations implement cloud security best practices like just-in-time (JIT) access and zero standing privileges (ZSP) to prevent security breaches and operational disruptions, while increasing efficiency and user productivity.

Learn more about us at www.britive.com

Email us at sales@britive.com

Reflectiz

Reflectiz is a leading cybersecurity solution provider and website digital security enabler. This enterprise grade solution protects online businesses from digital application risks, client-side threats like Magecart and web skimming attacks, web supply chain exploits, ex-domain risks, and more. For more information about how to gain control of your website security, visit the Reflectiz website.

Enso Security

Enso, an application security posture management (ASPM) platform, helps software security groups scale and gain control over their AppSec programs to systematically protect applications.
The Enso ASPM platform discovers application inventory, ownership and risk to easily build and enforce security policies and transform AppSec into an automated, systematic discipline.

Ready to Eliminate AppSec Chaos? Learn more about us at enso.security

Grip Security

Losing the grip on SaaS Security: The rapid adoption of SaaS within enterprises created a new set of security challenges that are missing adequate solutions. Grip offers a new approach to SaaS security, enabling organizations to discover nearly 100% of the SaaS applications used (known and unknown), govern, monitor and secure employee access and usage from any device and any location, and prevent data loss.

Learn more on how you can get a Grip on your SaaS Security at https://grip.security

Qrypt, Inc.

Founded by Kevin Chalker and Denis Mandich, Qrypt is the leader in cryptographic quantum security solutions enabled by Quantum Entropy-as-a-Service (EaaS). The company is dedicated to democratizing quantum cryptography to protect and defend our collective privacy from exploitation. Via strategic investments in cutting-edge quantum hardware companies, and exclusive partnerships with premier global research institutes and U.S. national labs, Qrypt has amassed multiple quantum entropy sources to create high-quality random keys at scale. Thanks to this technology and a team of seasoned leaders in engineering, physics, and cryptography, Qrypt has developed the only cryptographic solution capable of securing information indefinitely with mathematical proof as evidence. With more partnerships and deals in the works, Qrypt's mission is to become the world's security standard for the quantum age and beyond.

For insights into Qrypt's suite of solutions that help organizations prepare for the age of quantum computing, please visit www.qrypt.com.

Rezilion

Rezilion is an autonomous cloud workload protection platform that makes production environments self-healing and resilient to threats. Founded by serial cybersecurity entrepreneurs Liran Tancman and Shlomi Boutnaru, Rezilion secures vast environments with minimal manpower by integrating security into existing DevOps and IT automation workflows. To learn more, visit https://www.rezilion.com/.

Sepio Systems

Founded in 2016 by cybersecurity industry veterans, Sepio HAC-1 is the first zero trust hardware access platform that provides visibility, control, and mitigation to C2C, Zero Trust, insider threat, BYOD, IT, OT and IoT security challenges. Sepio's hardware fingerprinting technology based on physical layer data, discovers all managed, unmanaged and hidden devices that are otherwise invisible to all other security tools. Sepio is a strategic partner of Munich Re, the world's largest reinsurance company, and Merlin Cyber, a leading cybersecurity federal solution provider.

Closing call – "Learn more about us at https://sepio.systems and email social@sepio.systems anytime."

Cythereal

Cythereal's purpose is to secure businesses worldwide from the rising threat of targeted cyber-attacks, so they can focus on what they do best run their business. Our vision is to neutralize the attacker's asymmetric advantage by extracting intelligence from the attacker's failed attempts using the most recent advances in mathematical and statistical reasoning.
Our mission is to be the leader in predicting and preventing advanced malware based attacks by leveraging code sharing and reuse in malware. Our products and services are developed on research that was sponsored by the US Department of Defense and independently evaluated by MIT Lincoln Labs. Learn more about us at https://www.cythereal.com

Closing call – "Learn more about us at https://sepio.systems and email social@sepio.systems anytime."

uQontrol

uQontrol is an early-stage technology company focused on creating more secure, rich and intuitive online experiences putting consumers back in control. uQontrol believes individuals – not corporations or clouds – should have more control over their own information and that digital interactions should be more secure and reflecting the best experiences in the real world. Combining a passion for consumer control with extensive payment card security expertise, uQontrol created its first product – the Qkey. The Qkey is a radically simple new way to shop online and secure personal data with a more intuitive user experience and the latest Chip and PIN technology used by Visa and MasterCard. Qkey enables consumers to "load and lock" their personal information on the Qkey without remembering passwords, entering web site addresses, filling out forms or worrying about security. uQontrol will be distributing Qkey in the US and will be seeking international distribution partners in the coming months. For more information, please visit uQontrol.com or Qkey.com.

Satori

Satori created the first DataSecOps platform which streamlines data access by automating access controls, security and compliance for the modern data infrastructure. The Secure Data Access Service is a universal visibility and control plane that allows you to oversee your data and its usage in real-time while automating access controls. Satori integrates into your environment in minutes, maps all of the organization's sensitive data, and monitors data flows in real-time across all data stores. Satori enables your organization to replace cumbersome permissions and acts as a policy engine for data access by enforcing access policies, data masking, and initiating off-band access workflows.

Learn more about Satori at: www.satoricyber.com or contact: contact@satoricyber.com

Finalists for Top 10 MSSPs 2021

Atos	**www.atos.net**
BT Security	**www.ibm.com**
Wipro	**www.wipro.com**
Infosys	**www.infosys.com**
ECS Federal, LLC	**www.ecstech.com**
F- Secure Corp.	**www.f-secure.com**
Verizon Managed Security Services	**www.verizon.com**
Kroll	**www.kroll.com**
DeepWatch	**www.deepwatch.com**
NetSurion	**www.netsurion.com**

Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space. www.atos.net

BT Security

IBM is a leading global hybrid cloud and AI, and business services provider. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. Nearly 3,000 government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and business services deliver open and flexible options to our clients. All of this is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity and service.

For more information, visit www.ibm.com

Wipro

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 200,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

To learn more about us, please visit; https://www.wipro.com/

Infosys

Infosys is a global leader in next-generation digital services and consulting. We enable clients in 45 countries to navigate their digital transformation. With over three decades of experience in managing the systems and workings of global enterprises, we expertly steer our clients through their digital journey. We do it by enabling the enterprise with an AI-powered core that helps prioritize the execution of change. We also empower the business with agile digital at scale to deliver unprecedented levels of performance and customer delight. Our always-on learning agenda drives their continuous improvement through building and transferring digital skills, expertise, and ideas from our innovation ecosystem.

Visit www.infosys.com to see how Infosys (NYSE: INFY) can help your enterprise navigate your next.

ECS Federal, LLC

IBM is a leading global hybrid cloud and AI, and business services provider. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. Nearly 3,000 government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and business services deliver open and flexible options to our clients. All of this is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity and service.

For more information, visit www.ibm.com

F- Secure Corp.

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats. Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need.

Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure | linkedin.com/f-secure

Verizon Managed Security Services

Managed Security Services—Premises provides monitoring and management for a wide array of security devices at your various locations. Your devices are connected via a Connection Kit to a hosted Local Event Collector in one of our Security Management Centers. This vendor-neutral service allows you to select world-class products, help protect past investments in technology, and avoid vendor lock-in. For more information, visit www.verizon.com.

Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

DeepWatch

deepwatch helps secure the digital economy by protecting and defending enterprise networks, everywhere, every day. deepwatch leverages its highly automated cloud-based SOC platform backed by a world class team of experts who monitor, detect, and respond to threats on customers' digital assets 24/7/365. deepwatch extends security teams and proactively improves cybersecurity posture via its Squad delivery and proprietary Security Maturity Model. Many of the world's leading brands rely on deepwatch's managed detection and response. Visit www.deepwatch.com.

NetSurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.

Finalists for Top 10 Cybersecurity Experts

Craig Goodwin	Cyvatar
Adam Crawford	Herjavec Group
Arun Lakhotia, PhD	Cythereal
Doug Chin	Herjavec Group
Eva Chen	Microsoft
Jennifer Wang	Vectra.AI
Matthew Hickey	Hacker.House
Michael Gorelik	Morphisec
Prashanth Kannan	Independent
Sounil Yu	JupiterOne
Nadav Arbel	CYREBRO
Glorin Sebastian	Ernst & Young (EY)

Finalists for Top 10 Women in Cybersecurity

Stephanie Simpson	**Cyvatar**
Tami Hudson	**Wells Fargo**
Sarah Ashburn	**Attivo Networks**
Wendy K. Thomas	**Secureworks**
Deborah Wheeler	**Delta Airlines**
Kara Sprague	**F5 Networks**
Ellen Sundra	**Forescout**
Ellen McLean	**eSentire**
Jenna Raby	**RiskIQ**
Jennifer Arcuri	**Hacker.House**

Finalists for Top 10 Chief Information Security Officers (CISOs)

Cherri Heart	CarMax
Brian Klenke	**Bath and Body Works**
Corey Epps	**CVS Health**
James Johnson	**John Deere**
Renato Kirchgatter	**General Electric**
Jon Moore	**Humana**
Brent Conran	**Intel**
Mike Hamilton	**Critical Insight**
Richard Flahaven	**Harley-Davidson**
Jennifer Watson	**Raytheon**

Women in Cybersecurity Scholarship Fund for Diversity and Inclusion

Inclusive in our awards, we not only have the Top 10 Women in Cybersecurity to share, we opened our second annual Women in Cybersecurity scholarship program. This year's winner is Olivia Gallucci:

"I am honored to be a recipient of the Cyber Defense Media Group Women in Cybersecurity scholarship. I plan to use this scholarship to continue my education in cybersecurity, computer science, and Free and Open Source Software (FOSS). This scholarship allows me to immerse myself in new research pursuits, advance my FOSS cybersecurity research, and contribute to developing open-source security initiatives at Rochester Institute of Technology like Open@RIT. I hope that my research will inspire others to pursue secure coding and contribute to FOSS."

About the Winner

Olivia A. Gallucci (@ivyhac) was named to Rochester Institute of Technology's (RIT) 2020-21 Fall and Spring Semester Dean's Lists. Gallucci is double-majoring in Computing Security and Computer Science, and minoring in Free and Open Source Software (FOSS) and Free Culture. Gallucci finished her freshman year with a 4.0 GPA and is a member of RIT's Honors Program (top 3% of RIT's student body). She is treasurer of RITSEC, RIT's Cybersecurity Club, and Vice President of RIT's Women in Cybersecurity (WiCyS) Chapter. Gallucci has participated in eight cyber cybersecurity competitions, presented eight cybersecurity talks, and sails on RIT's sailing team.

Gallucci has received multiple student scholarships: (ISC)2 Women's and Undergraduates' Scholarships, RIT's $17,500 Five-Year Renewing Presidential Scholarship, and Executive Women's Forum Black Hat Scholarship. She also received a scholarship to present her research, Effectiveness of Threat Mitigation in Layers of the Open Systems Interconnection Model, at the 2021 WiCyS International Conference in Denver, Colorado.

Gallucci is an intern at Deloitte Touche Tohmatsu Limited's 30 Rockefeller National Headquarters in New York City. She is also a research assistant for Open@RIT, where she is continuing a school-financed independent research project, Summaries and Annotated Bibliographies of Successful Free & Open Source Projects.

Gallucci's long-term goals include contributing to FOSS security projects, volunteering for FOSS licensing compliance initiatives, and exploring secure coding practices to help bridge the gap between cybersecurity and software development. She hopes that her contributions to FOSS cybersecurity programs will increase transparency, trust, and security.

For More Information:

https://oliviagallucci.com

www.linkedin.com/in/olivia-gallucci

with her award, she has received an opportunity for a part-time internship with CDM as a cybersecurity reporter and blogger. Reach out to her with story ideas:

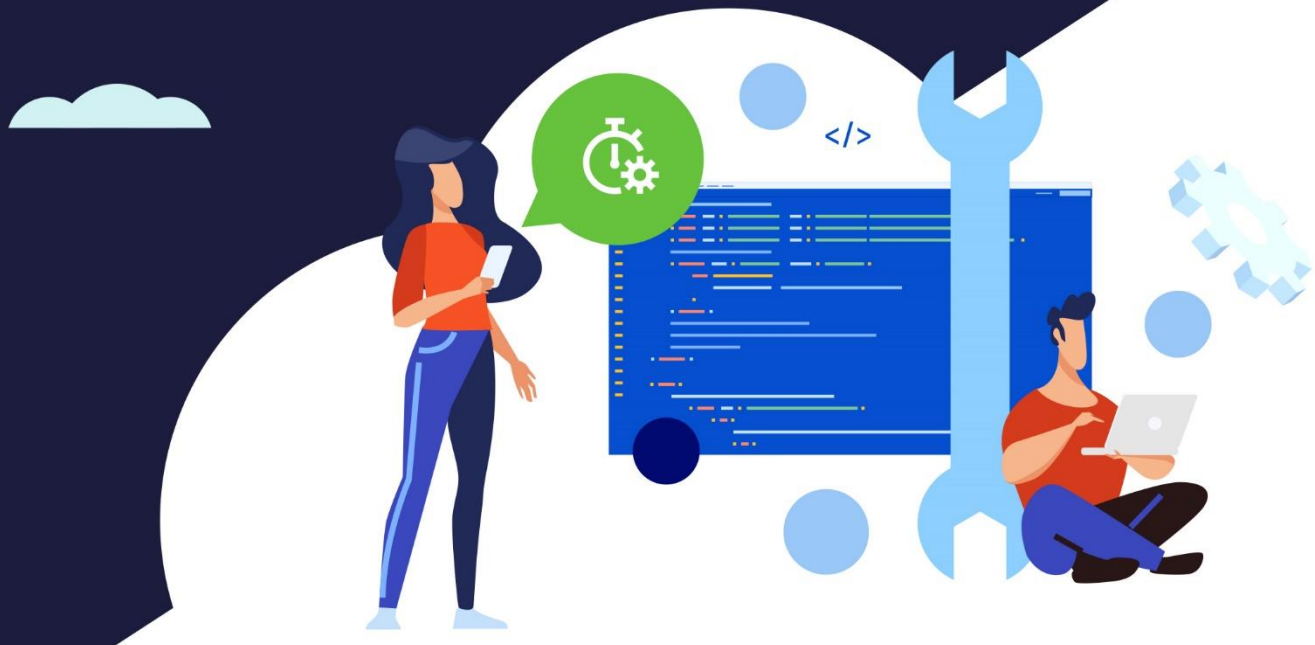
olivia.gallucci@cyberdefensemagazine.com

ANITIAN

Get to market 80% faster. Do it for 50% of the cost.

Give your business and DevOps teams the fastest path to security and compliance for cloud apps with Anitian's pre-engineered Compliance Automation Platform and Secure**Cloud** DevSecOps Platform.

www.anitian.com




Thought Leadership Articles

Is The Cloud Leaving You Exposed?

Exploring the public cloud and addressing its unanticipated security challenges

By Chuck Slate, Lead Architect, Attivo Networks, Inc.

On a traditional network, user accounts are the main identity type and, therefore, the primary security focus. In the public cloud, the concept of identity is extended to any object with entitlements (permissions) to another object. This includes “non-human” identities like applications, containers, virtual machines, and other object types that have historically played the role of a resource only.

A core benefit of the public cloud is that it offers managed services such as database, DNS, and storage services. Managed services free admins from the responsibility of having to build and maintain substantial pieces of the cloud infrastructure for themselves. Instead, they define a database table, for example, and grant access to the applications that need it. (In such a scenario, the applications function as non-human identities vis-à-vis the managed database because they have permissions to read or write to the managed database’s table.)

The sheer volume of cloud identities and entitlements resulting from new concepts like non-human identities and managed services can leave cloud security professionals overwhelmed and often blind to the full extent of their exposure.

The Wild West of Identities and Entitlements

What might amount to hundreds of identities on a traditional network could translate into thousands in the public cloud. That increase in the number of identities exacerbates existing security challenges. For example, “privilege creep” is the idea that identities accumulate access to more resources than they need over time. This situation has historically been a common problem on traditional networks. Because the public cloud has that many more identities, privilege creep is that much more probable and dangerous in

the public cloud. The public cloud has also seen an increase in the number of relationships between objects and, consequently, the number of entitlements. On a traditional network, for example, a user may have access to an endpoint. In the public cloud, that same user may have access to a virtual machine, which may, in turn, have access to an application, which may then have access to an API, a database, and a storage bucket.

The public cloud also introduces a unique set of identity-specific obstacles. For example, many corporations have a multiple-cloud strategy, and using multiple accounts within a single cloud platform is standard. As a result, there is no native way to assess an enterprise-wide security posture or view assets across platforms from a single management console. Moreover, organizations routinely sync identities from their local Active Directory with the public cloud to provide single sign-on services for seamless access to local and cloud resources alike. To understand the risk associated with Active Directory and public cloud integration, one needs only to consider the SolarWinds breach, which started with an on-premises compromise and led to the exfiltration of public cloud data.

The larger the public cloud footprint, the harder it is to track the set of cloud identities and their relationships with other cloud objects. Without proper visibility, accurate risk assessment and mitigation is an uphill battle.

A New Frontier

Developers did not design traditional IGA and PAM solutions for the public cloud, so they struggle to address its unique security challenges. Existing CSPM, CWPP, and CASB tools address specific aspects of cloud infrastructure security, but they generally lack identity-centric analysis and access controls. Manual methods to ensure a least-privilege approach to cloud security do not scale in an environment with large quantities of identities and entitlements.

Existing security paradigms do not inherently address the needs of cloud identity security, and a new segment of the security market has recently emerged in response to this blind spot. Industry analysts have created new acronyms to describe it, including Cloud Infrastructure and Entitlements Management (CIEM, pronounced “Kim”) and Cloud Permissions Management (CPM).

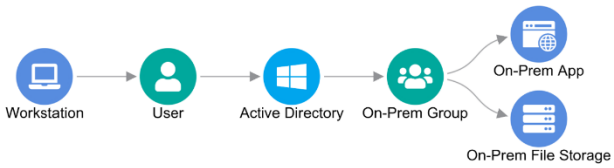
The common goals among the solutions in this budding sector can be summarized as follows:

1. Discover all cloud identities, cloud resources, and the entitlements between them
2. Support multiple cloud accounts and multiple cloud platforms in a consistent fashion
3. Provide graphical analysis of the relationships cloud objects have with each other
4. Highlight risky privileges and entitlement changes to critical cloud assets
5. Enable clear and straightforward action to mitigate risk and reduce exposures

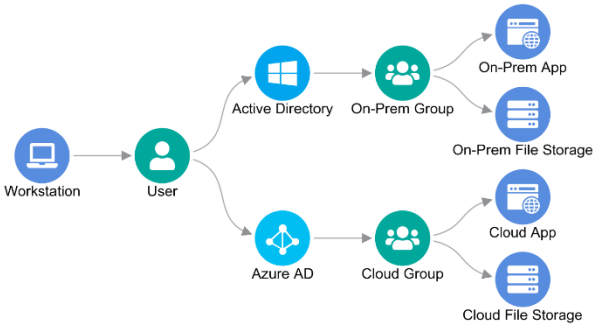
More to Cloud Security Than Just the Cloud

Most offerings in this nascent space focus exclusively on managing identities and entitlements in the cloud itself. As previously mentioned, however, the SolarWinds breach is an excellent example of an identity attack that exploited and manipulated both on-premises and cloud identities alike. In the end, cloud-specific visibility is only one piece of the larger security puzzle.

An attacker compromising a workstation on a traditional network, for example, can exploit its user credentials to access Active Directory and its resources.



When Active Directory credentials have been synchronized with the public cloud, that same attack has many more vectors available and can therefore do that much more damage.



A Comprehensive Approach

Installing a cybersecurity solution that performs analysis on public cloud identities and entitlements alone is like buying a home security solution that only puts a camera on the front door. In both cases, the solution cannot achieve its intended goal because it does not have the visibility it needs to adequately assess and mitigate risk for all possible attack paths.

For comprehensive protection, a solution must have a focus on identities and entitlements across the board. Specifically, it must be able to:

1. Intake and analyze identities and entitlements from endpoints
2. Intake and analyze identities and entitlements from Active Directory
3. Intake and analyze identities and entitlements from multiple public cloud platforms and accounts
4. Correlate the analysis results across the data sources and display them in a complementary fashion on a single pane of glass

As corporations continue to move to the public cloud, they must adopt a technology that provides a thorough analysis of their cloud identities and entitlements. That technology must, in turn, be part of a more extensive solution that monitors and protects identities and entitlements throughout the entire enterprise.

About the Author

Chuck Slate holds the role of Lead Architect at Attivo Networks. Chuck has over 25 years of experience building security solutions with expertise in computer networking and UI/UX design and development. Chuck earned his master's degree in Computer Science from Boston University. Chuck Slate can be reached online at (chuck.slate@attivonetworks.com, https://www.linkedin.com/in/chuck-slate/ and at our company website http://www.attivonetworks.com

The Future of Cybersecurity? Just One Word: Automation

By Dr. Peter Stephenson

If you are not better informed, smarter, better equipped, and faster than the adversary, you can count on your system being compromised at some point. When I'm asked about the future of cybersecurity, I generally recount a cautionary tale. As far as I know, this is never actually happened. But it brings into focus two of the most important concepts in cyber adversary threats: autonomous bots and blockchain.

Imagine the following scenario: it's late on a Friday evening starting a long weekend. There is a single engineer in the network operations center and a single engineer in the security operation center. Everything is quiet until the network engineer notices thousands of accounts logging in and removing money using the on-line banking system. At the same time, the security engineer notices the logins but sees nothing irregular about them except for their volume. The network engineer is concerned, and she disconnects the remote banking system from the Internet. At that point the security engineer notices that the attempts at removing money from accounts continue from inside the network but because the network is not connected to the Internet the attempts fail.

Neither the network engineer nor the security engineer can explain the sudden removal of money from so many accounts. Further investigation shows that there were several million dollars removed from a few thousand accounts in the space of less than five minutes. The security engineer notifies the forensic team, and they began to try to figure out what happened. Unusually there is absolutely no indication of a breach. However, late on a Friday night is not when one would expect millions of dollars to be removed legitimately from several thousand accounts at the same time. The engineers and forensic specialists can offer no explanation.

Here's what happened. Over the space of several months an autonomous bot from a hive net slowly accessed the protected network multiple times. The single bot was released, through phishing, into the network. That bot slowly sent account credentials to port 443 (https) via a blockchain network where they were saved. Once enough credentials were harvested, the bot destroyed itself leaving no trace. Because it was connected to port 443, the exfiltration was not noticed but was considered normal network operation. It set off no alarms in the intrusion detection system.

The intrusion detection system was a next-generation system using machine learning. However, prior to penetrating the network, the hive net attacked the network multiple times in multiple ways collecting the intrusion detection system's responses. From those responses, the hive crafted attacks that would not trigger the intrusion detection system. This type of machine learning black box attack is called "querying the oracle". From the information gained, the first bot was able to enter the network as part of a phishing campaign. A second set of attacks, triggered inside the protected network, allowed the bot to query the oracle internally. The hive now had all the information it needed to complete the attack.

Having gathered the defense information, the hive now could exfiltrate money from accounts without being detected. On the Friday evening the hive, using its swarm bots, performed a smash-and-grab attack. Spoofing legitimate user accounts, the swarm logged in and transferred money out via the blockchain network. Each bot destroyed itself after performing its mission. The block chain network terminated in a bitcoin wallet. Money in the bitcoin wallet immediately was transferred to several additional bitcoin wallets, obfuscating the trail. The money was never recovered.

This is an example of an attack by autonomous bots. In other words, the bots do not report to a hive master or a bot master. Unlike current generation attacks, the hive master simply needs to give the hive its objective and let the hive operate autonomously. The bots learn from each other and the intelligence of the hive grows.

In current generation attacks, the bot master manages a command-and-control server. From there he directs the bots to attack. Autonomous bots, however, receive their initial programming and receive initial commands from the hive. The hive and the bots are based upon machine learning or other forms of artificial intelligence and do not require human intervention once they're programmed and their objective defined.

So how do we defend against autonomous hives and swarm bots? The only answer is that we must deploy machine learning models that learn from attacks against them - in addition to known attacks - and develop defenses on the fly. That means we must be smarter, faster, and more alert than current generation tools are. What does that really mean? It means that in the future humans will not be fast enough to respond. In fact, for certain types of current, distributed attacks humans are not fast enough to respond. Lest you interpret this as "there is no place for humans in cyber security", let me state clearly that you are about half right.

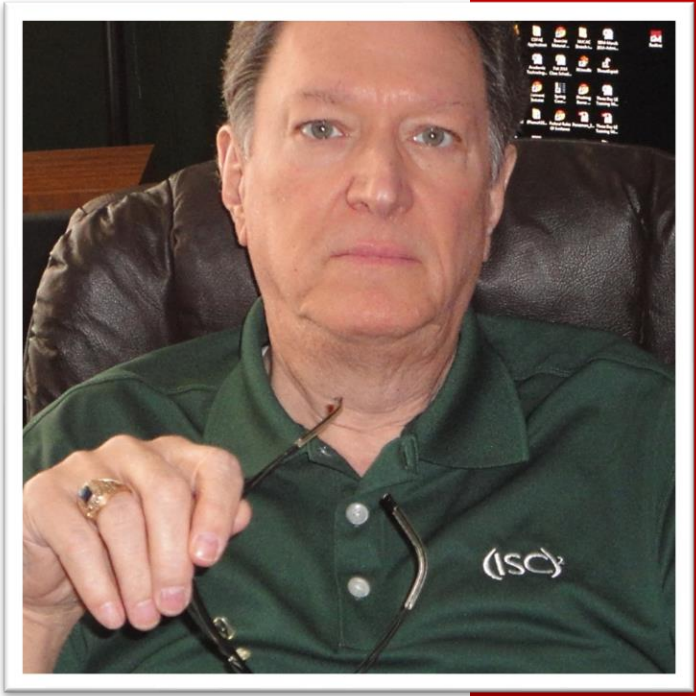
Humans always will make the hard analytical decisions. To turn over all cyber security to an algorithm would eviscerate human control and open the way to errors and bias in the machine learning (ML) code. However, there are certain functions that depend upon rapid response - often at wire speeds - that preclude human intervention until the event is interdicted and it's time for after-action analysis. Then, using analytical tools, humans enter the picture and make decisions that then are added to the training set. In addition, ML systems often add events to their training set on their own.

Here's the point… cyber security in the future must become a partnership between people and machines. There are things that the adversary will do with ML that a human can't hope to recognize and interdict in a timely manner. But there also are things on which the human and the machine can - and must - collaborate. The old saw that computers do only what their human programmers are telling them to do. Today - and, certainly, tomorrow - machines will learn to program machines with little to no human interaction. While it

may be true that there is a human at the start of this chain, it also is true that at some point the human contribution is minimized to the point of obscurity. That is, potentially, a dangerous time for cyber security.

Imagine, for example, a hivenet created by an especially talented hacker with malicious intent. The hive wanders through the Internet achieving its mission as assigned by its hacker hive master. But all the time it's doing the human's bidding, it is learning and training the swarm bots' ML. At what point - if any - do the swarm bots and the hive thumb their virtual noses at the human and go their own way? Does this mean that the future of cyber security is an endless battle of the bots with the bots becoming ever-more sentient? That is a debate for cyber philosophers, not security professionals. But - and this is a big but - what would we do if that became the case?

About the Author



Dr. Peter Stephenson has reactivated himself to exclusively focus on deep next generation Infosecurity product analysis for Cyber Defense Magazine after more than 50 years of active consulting and teaching. His research is in cyber-legal practice and cyber threat/intelligence analysis on large-scale computer networks such as the Internet. Dr. Stephenson was technology editor for several years for SC Magazine, for which he wrote for over 25 years. He is enabled in his research by an extensive personal research laboratory as well as a multi-alias presence in the Dark Web. He has lectured extensively on digital investigation and security, and has written, edited or contributed to over 20 books as well as several hundred articles and peer-reviewed papers in major national and international trade, technical and scientific publications. He spent ten years as a professor at Norwich University teaching digital forensics, cyber law and information security. He retired from the university as an Associate Professor in 2015. Dr. Stephenson obtained his PhD at Oxford Brookes University, Oxford, England where his research was in the structured investigation of digital incidents in complex computing environments. He holds a Master of Arts degree in diplomacy with a concentration in terrorism from Norwich University in Vermont. Dr. Stephenson is a full member, ex officio board member and CISO of the Vidocq Society (http://www.vidocq.org). He is a member of the Albany, NY chapter of InfraGard. He held – but has retired from – the CCFP, CISM, FICAF and FAAFS designations as well as currently holding the CISSP (ret) designation.

The Silver Bullet for Ransomware's Golden Goose

Ransomware is a hugely profitable business. The only way to end it is to stop criminals from making money off your data.

By Elliot Lewis, Co-founder and CEO of Keyavi Data Corp.

It's every CEO's worst nightmare: You report to work early one morning only to find your computers frozen, your essential data locked and an ominous message from cybercriminals demanding an outlandish ransom to restore them. In the meantime, your employees can't work, your customers can't buy your products and you're bleeding revenue by the minute.

Could it happen to you?

Unfortunately, the odds are bad and getting worse. Between 2019 and 2020, attacks increased 62 percent worldwide and 158 percent in North America, according to cybersecurity firm SonicWall. The pandemic ushered in a new era of of remote and hybrid work – and with it, new opportunities for criminals to worm their way onto the corporate network through VPNs and remote desktop applications. Last year, 61 percent of companies were hit with ransomware. Nearly 300 have been attacked so far this year, earning cybercriminals at least $45 million. And those are just the attacks we know about.

No sector of the economy is immune. The more critical data is to organizations, the greater the leverage it offers to criminals, who have extended their sticky fingers from businesses to schools, hospitals – and with the Colonial Pipeline attack –national infrastructure.

Even if you don't pay the ransom, an attack represents a severe financial hit. Costs –including lost productivity, investigations and forensics, breach notifications and reputational damage – are rising at a clip of 30 percent a year, according to research firm Cybersecurity Ventures. By 2031, the organization predicts ransomware will cost companies $265 *billion*, with an attack occurring every 2 seconds.

What accounts for this stupendous rise in size and scale?

In a word, money. Technically, ransomware is just another form of malware, but financially, it's a juggernaut for criminals, who know that today's companies simply can't function without access to their data. In recent years, they've found ways to extract revenue from it long past the initial ransom demand. To understand and outsmart their lucrative business model, you need to examine the dynamics of an attack.

The Three Phases of Ransomware

Companies experience ransomware as a sudden, incapacitating hit – which of course is part of the plan. But for criminals, it's just the tip of the iceberg. Behind the scenes, they engage in many other activities, and not all of them make money.

Attacks are staged in three phases:

Phase 1 – Entry, reconnaissance and launch – a loss leader for attackers.
Criminals hop onto the corporate network by inserting malware into a phishing email or sending out a fake software update. They use rootkits and other tools to spy on users, scope out systems, escalate privileges, disable security software and – most importantly – find and steal the organization's most valuable data. Masking techniques allow them to snoop and filch data undetected for weeks or even months. Finally, at the end of Phase 1, they launch the file-encrypting ransomware. Only at this point do victims become aware that a problem exists.

Phase 2 – Making the victim pay: the cash to criminals starts flowing
Attackers attempt to extort companies by demanding payment to decrypt the victim's data files. Paying the ransom, however, doesn't end the problem. A Cybereason study found that while 46 percent of companies who pay a ransom to regain access to their data, some or all of it is corrupted. Much worse, though victims are unaware of it at this point, attackers may have made and kept copies of all the data the company just paid to restore. Decrypting files does not address this problem at all.

Phase 3 – Criminals make even more money from exfiltrated data: a wealth of recurring revenue opportunities.
The first attack is just the beginning. Eighty percent of organizations that pay a ransom go on to suffer a second attack, Cybereason found. Attackers threaten to publish their stolen data if companies don't pay another ransom, often upping the ante if they don't meet a specified deadline.

Ransomware today has evolved into a complex criminal enterprise involving a shifting, interlocking network of gangs and cartels, including Maze, LockBit and Ragnar Locker, which work together and on their own to make money through extortion and selling stolen data to third parties. Some, such as REvil, have even devised ways to make passive income, selling the tools of their trade to other criminals in ransomware-as-a-service franchises.

Anatomy of the Ransomware Business

In this ransomware business model, attackers expend time and resources but make no money in Phase 1. The cash flow starts with the direct victim ransom demands in Phase 2, but there's a catch. Companies with good, secure backups know they can get their systems up and running again, and may refuse to pay. Many mistakenly believe the attack is all about *unlocking* their data, and once they regain access to it, everything will be fine.

But attackers know they can count on Phases 2 and 3 – extorting companies for the same data (sometimes called double extortion) and/or selling it to others. They can do this because companies have no way of getting their data back after it's been stolen in Phase 1.

Once companies understand the predicament they're in during Phases 1 and 2, they're often willing to pay up. For example, meat producer JBS recently paid an $11 million ransom *after* its operations had already recovered from a ransomware attack. Why?
Their published statement said: "In consultation with internal IT professionals and third-party cybersecurity experts, the company made the decision to mitigate any unforeseen issues related to the attack and ensure no data was exfiltrated."

They paid $11 million to "ensure" that no data would be exfiltrated. But their only assurance was the word of a cybercriminal gang, which still has their data. Those criminals may someday decide that $11 million – or $21 million or $31 million – actually isn't enough. In fact, there's no limit to the number of times an attacker can come back and demand more money. Or sell stolen data to third parties. Or both.

The Heart of the Problem – A Flawed Security System

The JBS example illustrates a fundamental flaw in modern security systems: They can't ensure that sensitive data won't fall into the wrong hands. That simply isn't possible with current security protocols, which fall into two main categories:

1. Attempts to keep data contained. These include identity and access management systems, mobile device management, sensitive data encryption, cloud access management and secure storage. These are all important measures, but they're not perfect. An attacker only needs to get through one of these layers to penetrate the corporate network and steal data.

2. Forensics, monitoring and intelligence, including SIEM and SOAR. These solutions exist because the first solutions too often fail.

Companies are pouring a lot of money into these systems. Spending on cybersecurity and risk management is the top priority for CIOs and is expected to reach $150.4 billion this year, according to Gartner.

Many companies also purchase cyberinsurance, but as ransom amounts rise and governments crack down, insurers are getting pickier about issuing policies. Some, like European insurer AXA, may stop offering them entirely.

A Game-Changing New Cybersecurity Paradigm: Self-Protecting Data

Despite their best efforts, companies can't stop ransomware attackers from extracting and holding sensitive data, which is at the heart of their lucrative business model.
But what if data could protect itself? Then companies wouldn't have to spend millions of dollars in a vain attempt to keep it out of the hands of ransomware attackers – or try to trace it after they've already gotten hold of it.

In fact, the technology to do this exists today. Instead of trying to keep data contained, Keyavi encases it in multiple, industry-standard encryption layers with continually changing PKI encryption keys. It then infuses each of those layers with very specific governance policies and forensic capabilities.
That means sensitive data can safely travel anywhere – because everywhere Keyavi-infused data goes, it follows the rules of the individual or organization that owns it.
How does that work?

Example 1: A ransomware attacker compromises a privileged account – a typical tactic during Phase 1.

With traditional security systems*:* The company encrypts its sensitive data and has an identity and access management system in place, but these protections aren't effective enough. Once the attacker gains control of an account with high-level access privileges, he can access the authorized user's decryption keys, decrypt the data, export it, copy it ad infinitum, and send it wherever he pleases.

With Keyavi: Even though the attacker has successfully tricked the security system into believing he is the actual user via identity compromise, the built-in data protections will not allow him to decrypt and read it – much less copy it, export it or send it to others.
Why? Because policies are embedded in the data – policies that extend beyond just identity. As soon as the hacker tries to open sensitive data, it automatically asks itself, *Where am I? Am I allowed to be here? Why did I ever leave my owner's office?* And right away, this highly intelligent data realizes: *This is not a pre-authorized location. Therefore, I don't care who he says he is, I won't open in this location.*
And that's the end of it. No matter how many accounts the attacker hacks into or creates, no matter how many spying tools he uses or legitimate-looking requests he issues to access sensitive information, the data will refuse any access that is not authorized by company policies.

The data won't just sit there silently, either, but will capture full forensics of the attacker and his location, then send it to the data's rightful owner.

Example 2: An attacker has already stolen a company's data.

With traditional security systems: Even if the company pays a ransom to unlock its files, there's no guarantee it will ever get all copies of its data back. The attacker can return to make multiple extortion attempts or sell the data to third parties at any time.

With Keyavi: If data is stolen during a ransomware attack, whoever owns that data can revoke access anytime, anywhere at the mere touch of a button. This includes exfiltrated data that resides on an attacker's devices, websites or storage systems. The attacker, and anyone he sends it to, will never be able to see, access or use the data again.

Example 3: An attacker posing as a software consultant tries to copy sensitive data onto a USB drive.

With traditional security systems: Once the attacker leaves the premises, the data goes with him, never to return.

With Keyavi: Even if data has been copied onto a USB, the data's built-in protections will never allow itself to be opened on an unauthorized device for an unauthorized user at an unauthorized location.

These examples illustrate just a few of over 50 protective capabilities Keyavi can infuse into data. Policies can prevent data from traveling to devices that don't have specific anti-malware applications installed and running. They can prevent print screen screenshots or data-sharing on Zoom. They can apply different permissions, such as read-only or edit, to different users. Whoever owns the data can control and alter these policies at will, even if their data has already left their possession.

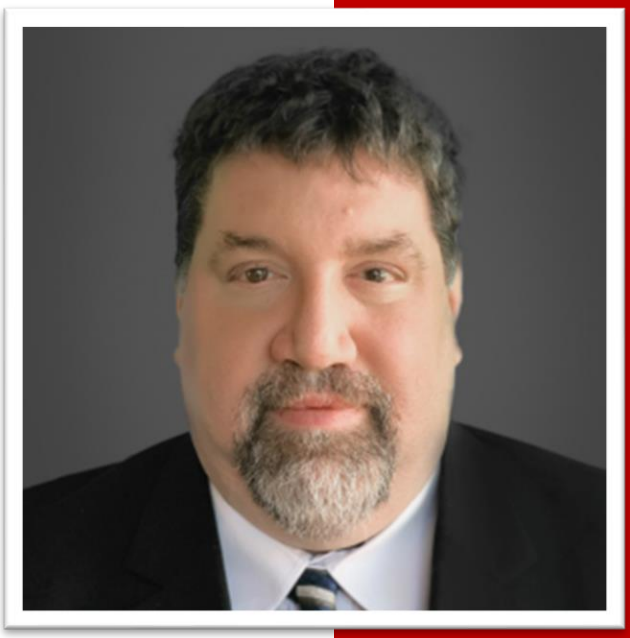
Keyavi's Silver Bullet

Unlike other security systems, self-protecting data strikes at the heart of ransomware's business model: its money-making machinery. If attackers can't demand extortion payments or sell data to third parties, their major sources of revenue dry up, and they remain stuck in Phase 1. While criminals may have broken into the mansion, if they can't take anything out, it does them little good.

Because most enterprises today have off-site backups, many will refuse to pay the initial demand to decrypt. For example, cloud storage company Spectra Logic and chip manufacturer MaxLinear refused to give in to extortion threats, even though both carried cyber insurance, which likely would have footed at least some of the ransom payments. Instead, they chose to get help from the FBI and work to restore their systems.

Criminals make so much money from selling and extorting companies for stolen data during Phases 2 and 3 that they can afford to skip Phase 1 extortion attempts if a company refuses to pay and move onto their next victim. But the advent of self-protecting data eliminates these sources of income – and with it, the incentives that draw most of the bad actors into this business. When attacks require the same amount of work, but become far less profitable, the motivation to launch them will fade, forcing attackers to turn their attention to other exploits.

To learn more about Keyavi's unique self-protecting data solutions, visit www.keyavidata.com.



About the Author

Elliot Lewis is an internationally renowned cybersecurity expert protecting some of the world's most valuable intellectual property – both as a security executive for Fortune 100 companies and as an industry, government and military advisor helping hundreds of customers solve their most challenging data security problems. Before launching Keyavi Data in 2020, Elliot held a number of leadership roles at technology companies such as Microsoft, where he ran the network security division of Windows, then became the senior security architect for the Security Center of Excellence for Microsoft itself. He was also director of strategic services at Cisco, served as chief information security officer (CISO) at Merrill Lynch worldwide and was chief security architect at Dell Corporation. A published author and sought-after speaker, Elliot is also the co-inventor of five network security patents for Microsoft and Dell. He can be reached online at elliot.lewis@keyavidata.com and through Keyavi's website at https://www.keyavidata.com

No, You Don't Need

By Daniel Petrillo , Director of Security Strategy, Morphisec

Endpoint detection and response (EDR) solutions, and their evolution -- extended detection and response (XDR) platforms -- are increasingly popular. To underscore that point, the market was valued at $1.81 billion in 2020, according to Mordor Intelligence, and looks to increase to $6.9 billion by 2026 for a CAGR of 25.6% over the next five years. This is huge as more companies start to look into adding EDR functionality, whether through buying software or buying managed services, into their security stack.

Vendors and industry analysts are paying attention, with Gartner expecting most endpoint protection suites to include EDR/XDR functionality in their platforms and more deals going toward blended solutions. Ultimately, the idea of detecting threats and responding quickly is now viewed as table stakes in cybersecurity. It goes along with the common idea that there's no way to prevent a breach, so you'd better be able to quickly stop and remediate it to limit the damage.

Here's the thing: this is no longer the case.

Most organizations cannot realize the full value of EDR solutions with their staff and budget, and the current market push among the vendor community does a disservice to resource-stretched IT and security teams. Outside of a few large companies with enough budget to staff up a security operations center, to be quite honest, EDR is even kind of useless. It also distracts from more effective and efficient ways to improve security.

Why EDR Became Important

Traditional antivirus solutions do one thing very well: block malware that has a known signature . What they don't do is block in-memory attacks or fileless malware; if there isn't a signature associated with it, traditional AV will be evaded. So-called "next-gen" AV that leverages machine learning is meant to close this gap, attempting to classify files as malicious or benign without the use of signatures. NGAV also doesn't do that very well, but that's a topic for a different article.

EDR/XDR tools are meant to add the extra layer needed to detect attacks that can't be prevented. They do this through continuous collection and interrogation of endpoints telemetry (and more in the case of XDR). Theoretically, when the EDR solution delivers an alert, the security team can investigate and decide whether or not to respond. If a response is required, the idea is that most damage can be avoided even after initial access into a network. Seems like a good idea, right?

With that idea in mind, the market grabbed hold of EDR/XDR as a solution class and began pushing it as a critical need in the corporate security stack. The problem is that EDR doesn't actually make your organization safer on its own; if anything, all it does is add more work for IT teams that are already overwhelmed and under-resourced.

Why EDR Won't Make You Safer

EDR solutions are not enough to actually defend against the kinds of advanced cyber-attacks that threaten your organization every day. The market agrees too. Sixty-five (65) percent of the companies who lack an endpoint detection and response solution, according to Ponemon, said they don't have one because it's not effective against new or unknown threats. Consider that AV-TEST has collected more than 1 billion distinct types of malware and potentially unwanted applications as of early 2021. There is no way that any solution can detect every possible variant with any reliability.

Beyond that though, is the substantial time-investment required to make EDR work. The average EDR/XDR solution generates 11,000 alerts every day. Each of those alerts can take upwards of 10 minutes to investigate and determine whether it's a false positive or not. Basic back-of-the-envelope math means that you'd need to hire 229 L3 analysts to work 8 hour shifts each day just to clear all those alerts.

EDR vendors recognize this, which is why managed detection and response (MDR) is now becoming more prominent. It's also a large enough issue that separate product categories, like security orchestration automation and response (SOAR) are often added to the stack, as a means of dealing with an overwhelming number of alerts. Not every company that wants to access EDR capabilities has the budget to pay for the software and then staff up a security operations center of highly paid analysts to investigate alerts all day. So they hire a managed service provider.

This doesn't do anything with the volume of alerts though. It's still 11,000 alerts to sift through and determine which of them are real attacks and which are false positives. This creates security alert fatigue, a growing problem when 70% of IT leaders have seen the volume of security alerts they receive more than double since 2015.

There is no way to sift through all of those alerts to find the attacks that are real, and in fact threat actors are likely banking on that problem. It's incredibly easy to confuse even the best machine learning algorithms, and even so-called "predictive" analytics software still needs to be updated with signals from

existing attacks. A true zero day is likely to bypass these detection-centric tools just as much as it sails past traditional signature-based antivirus programs based on file scanning.

What to Do Instead of EDR

EDR is a great idea, but honestly most companies don't need one. They don't have the budget to fully staff up a SOC, or even hire dedicated security staff, and MDR services are pricey to access and offer limited value. What then is a company with limited budget for security -- e.g., everyone outside the Fortune 500 -- to do when they must protect themselves from fileless attacks, exploits, supply chain, and other living off the land attacks that regularly bypass antivirus?

What most companies need to do first is focus on the basics of IT hygiene: deploying patches on all their critical software, applying the principles of least privilege, leveraging native OS tools to secure their endpoints, and ensuring that they're training employees on security awareness.

A strong patch/vulnerability management program can mitigate 14 techniques in the MITRE ATT&CK framework, spread throughout phases like Initial Access, Defense Evasion, and Lateral Movement. This is more than double the six techniques mitigated by NGAV/AV technologies, and more effective by far than trying to detect attacks in progress -- especially when most modern attacks include a defense evasion component.

It's also a common pathway for attackers. A study from 2019 found that in 60% of the attacks examined, adversaries took advantage of a vulnerability that could have been patched … but wasn't. There are a lot of reasons why companies don't patch as frequently as they should; the reality is that getting better at patching still improves your security far more than any detection tool.

More interesting though is that 30 techniques in the MITRE framework are mitigated solely by applying the principles of least privilege. Estimates suggest that nearly 80% of all attacks use privilege escalation in some capacity. What this means in practice is that you could put substantial barriers in the way of a high number of cyberattacks just by ensuring that admin privileges are suitably limited within the organization.

But reduced risk of privilege escalation isn't the only benefit of careful privileged account management. Using MITRE's free ATT&CK Navigator, privileged account management can mitigate dozens of techniques across most tactics, including initial access, execution, persistence, and more. The best part about this is that privileged account management is a free action that every company can take right now.

Security awareness training and leveraging native OS tools are the other two big free actions that companies can take right now. For Windows users, Microsoft has spent $1 billion a year since 2016 improving their cybersecurity capabilities. Many of those are already built into Windows 10, and they're as good as the third-party solutions that you pay for. They even already include behavior-based analysis and machine learning, meaning they have feature parity with other solutions too.

There are some diminishing returns in security awareness training, unfortunately, with some reports saying that 3% of your employee base will click on a phishing link no matter how much training they have. That doesn't mean don't do it though. You can still substantially cut down on the risk of initial access with a regular education program on how to recognize scam emails and having an informed user base.

Final Thoughts

EDR/XDR platforms are great tools for the companies with enough budget to staff them correctly or hire someone else to do it for them. They're not a silver bullet -- nothing in cyber is, really -- and in most cases they're not even necessary for better protection. Honestly, buying an EDR tool without having the resources to properly use it is like purchasing a yacht when you don't have the money to hire a crew for it.

Sure you own a yacht now, but without a skilled crew it's not doing anything other than sitting in drydock. What most companies need is to go back to basics and ensure they've done the fundamentals. Then and only then can they go for the next phase and seek out protection from evasive modern attacks through extending their zero trust strategy fully to the endpoint (a topic for another article).

About the Author

Dan Petrillo is the Director of Security Strategy for Morphisec. Dan's years of experience in cybersecurity strategy began when he was the Product Manager for an Industrial IoT company that needed to figure out a way to secure the IoT devices and software that remotely controlled the lighting and machinery for manufacturing facilities. This eventually led him to work for Cybereason just before taking his current position with Morphisec. Dan attended Northeastern University for his bachelor of science degree in Electrical Engineering. Dan can be reached on LinkedIn and at our company website www.morphisec.com

APIs are the New Cybersecurity Battlefield, But You're Doing It Wrong

By David Thomason, WW Director of Solution Architects at Noname Security

"For every complex problem there is an answer that is clear, simple, and wrong."

- *H.L. Mencken*

Before the global COVID-19 pandemic, Gartner predicted that APIs would become the most-frequent attack vector by 2022. Necessity, as they say, is the mother of invention. The pandemic forced many to accelerate their digital transformation journey. Enterprises had to rethink the perimeter, transition to supporting an almost entirely remote workforce, and adopt multi-cloud infrastructure — APIs became the lifeblood of the modern digital enterprise.

This rapid shift to an API-first world also accelerated API cyber attacks. It's safe to say that APIs are already the most-frequent attack vector ahead of schedule, establishing API security as one of the top initiatives for CISOs worldwide.

Yes, APIs are under attack, but I caution security leaders of the dangers of treating the symptom instead of the cause of API vulnerabilities. *API security is far more than just attack prevention.*

Many of the recent API leaks, like Experian leaking American credit scores or Peloton leaking user data, were not due to an attack. A single misconfigured API can put an entire environment at risk. *API security is not about protecting APIs, it is about protecting an enterprise's digital environment from the threats associated with APIs.*

What is API Security?

It is critical that we look at API security through a broader lens. For example, simply implementing a solution to address the OWASP API Security Top 10 is the equivalent of a stick house. It's a step in the right direction, but ultimately leaves a false sense of security. I submit the following as a more accurate and strategic definition of API security:

> *API security refers to protecting the integrity of your digital environment from API vulnerabilities, API misconfigurations, and API cyber attacks.*

It may seem like semantics, but in practice there is a significant difference between having an API security strategy that focuses solely on a "shift-left" approach, or one that only reacts to attack patterns and an API security strategy that proactively eliminates vulnerabilities and resolves misconfigurations before they can be exploited.

Let's explore a proactive and pragmatic approach to API security that can help eliminate risks associated with APIs.

D.A.R.T - The Proactive API Security Strategy

D.A.R.T. is an acronym that stands for Discover, Analyze, Remediate, and Test. These are the 4 pillars of an API security strategy designed to protect your entire digital environment. D.A.R.T. serves as both a way to view the challenges associated with your APIs as well as a way to measure your existing API security efforts.

The 4 pillars of D.A.R.T. have an interdependent relationship with each other, and your overall API security posture will only be as strong as your weakest link. I'll define each pillar of the D.A.R.T. API Security Strategy:

Discover

Discover refers to the ability to find and inventory **all** APIs. Most enterprises don't know how many APIs they have. And many legacy and rogue APIs slip through the cracks and aren't even routed through an API gateway or WAF. In our experience, we've found that around 30% of APIs are unknown and unmanaged. These blind spots pose a significant threat to the business.

Additionally, most organizations don't have visibility into the data and metadata associated with their APIs. Questions like "Which APIs send/receive sensitive information like credit card numbers or social security numbers?" and "Which APIs are private and which are public?" are a lot harder to answer than you would imagine.

Without a complete inventory of APIs and a catalogue of the associated data and metadata, you really don't know what you need to protect, and your environment is at risk. API discovery is the critical first step of API security.

Analyze

Analyze refers to the ability to detect API vulnerabilities, misconfigurations, and attacks. As I mentioned earlier, your ability to analyze APIs is directly related to how effective you are at discovering APIs. Without a complete inventory or APIs and the associated data, it is impossible to analyze the access, usage, and behavior of your APIs.

There are many tools out there with good attack detection, but it is also important to analyze the configuration of every device, physical or virtual, that touches the APIs, to ensure APIs are operating only as intended. Your digital environment is more secure when you find and fix mistakes before they are exploited. That leads me to the next pillar of the strategy.

Remediate

Remediate refers to the ability to resolve misconfigurations and prevent attacks. Again, your ability to remediate vulnerabilities is directly related to how effective you are at discovering and analyzing your APIs.

You need to have a means of blocking attacks in real-time, as well as integrating with existing remediation workflows and security infrastructure. This opens the door to a world of remediation options — from automatically generating a Slack or Jira ticket to revoking the credentials of a misbehaving user or just simply blocking the IP address of a bad actor. Even the simplest integration (e.g. Slack notifications) can offload much of the manual efforts required by the security team to deal with both legitimate and false-positive events.

Test

Test refers to actively testing your APIs to validate confidentiality, integrity, and availability before and after they are deployed to production. Most applications are tested, most APIs are not. And given the dynamic nature of APIs, it is critical to have routine, active testing to ensure that your environment remains secure as API policies and behaviors change.

Conclusion

APIs are a leading cyber security threat to businesses; however, focusing only on either “shift-left” or API attack prevention is a dangerously narrow view. Security organizations need to think more broadly about API security. The goal isn’t to just protect an API from an attack, the goal is to protect your entire digital environment from all API threats, ranging from cyber attacks to simple misconfigurations. This broader mindset, guided by the D.A.R.T. API Security Strategy will help enterprises secure their environments across the entire software development lifecycle.

About Noname Security

Noname Security protects APIs in real-time and detects vulnerabilities and misconfigurations before they are exploited. Easily resolve API vulnerabilities across 4 key pillars — Discover, Analyze, Remediate, and Test — with a completely out-of-band solution. You don't deploy Noname, you simply connect it.

Fortune 500 companies trust the Noname API Security Platform to protect their environments from API attacks, vulnerabilities, and misconfigurations. Noname is a privately held company headquartered in Palo Alto, California, with an office in Tel Aviv. www.nonamesecurity.com

About the Author

David Thomason started his career in computer security working in the United States Air Force, serving the Air Intelligence Agency including the Air Force Information Warfare Center (AFIWC) and the Air Force Computer Emergency Response Team (AFCERT). While working as an incident response team lead for the AFCERT, David was the first person to have three hackers apprehended in separate security incidents. Since then, David has provided security services including incident response, risk assessments, penetration tests, and security deployments for dozens of companies. In 2012, David was responsible for the apprehension of a fourth attacker who was stealing SmartGrid technology from a US utility company. In 2019, David joined NSS Labs as principal researcher/architect. In November of 2020, David joined Noname Security as employee #3 in the US and leads the WW team of Solution Architects. David can be reached online at dt@nonamesecurity.com, on LinkedIn (https://www.linkedin.com/in/dthomason/) and at our company website http://www.nonamesecurity.com

Taking Back Control of Today's Software Supply Chain

By Jasmine Noel, Senior Product Marketing Manager, ReversingLabs

Supply chains are under attack. Malicious actors perpetrating these breaches will continue to succeed until security teams abandon common myths and misconceptions around these risks in favor of a more holistic fact-based approach.

While this threat has existed for a long time, the focus on supply chain attacks has grown in intensity just recently. It started late last year with the SolarWinds SunBurst attack and was followed by a steady stream of attacks in early 2021, including Microsoft Exchange and Codecov. In fact, according to the Identity Theft Resource Center (ITRC), supply chain attacks in the U.S. rose by 42% in Q1. Since then, they have continued with the latest attack taking place just recently over the July 4 holiday against IT management software vendor Kaseya.

There are several reasons why businesses remain susceptible, which include four key misconceptions that undermine software development and open the doors for costly attacks. A new Interos Annual Global Supply Chain Report, reveals that global supply chain disruptions caused by breaches, as well as COVID-19 and the Suez Canal incident, cost large companies, on average, $184 million a year. The report also found that 83% of businesses have suffered reputational damage because of supply chain problems.

The good news is that businesses are looking more seriously at defending themselves against supply chain attacks. A ReversingLabs study found that awareness is up with 52 percent of respondents believing that securing against supply chain attacks is needed. Less promising, however, are findings that show 30 percent of respondents are not confident that software is being released and accepted without malware.

This brings us back to the myths and misconceptions that help to perpetuate the issue of a vulnerable supply chain. Let's take a look at the four most prevalent myths that continue to prevail throughout the industry, and explore why they are not true, how teams can reverse course, and what solutions are available to help businesses take charge right now.

Myth 1: Scanning Source Code is Enough

While it is true that source code analysis is effective, this really only applies to assessing the quality of written code for vulnerabilities early on. Here's the challenge. Much can happen across the entire development process where multiple owners and software components introduce gaps and risks. This happens when they add and modify source code, which they assume is secure simply because it's coming from a trusted source.

These actions immediately open the door for threats and attacks, more of which are originating from these unconventional sources. For SolarWinds the source was a build server. Further complicating matters is that static and dynamic scanning don't deliver a complete view of how malicious software packages can behave and if software is already compromised, SAST/DAST/SCA and VM won't help.

The action here is for businesses to begin assessing all software components beyond known vulnerabilities using a more comprehensive and automated scan process across repositories and libraries.

Myth 2: You Only Need to Scan Binaries for Malware with AV

Today's modern software packages and installers operate outside the scope of many AV and other scanners. This includes application security tools. In addition, many files are simply too large or have components, such as containers, that extend beyond the scope of these scanners.

Currently there is no known signature for novel backdoor malware, which is malware that is well-hidden and obfuscated within the code base and can bypass normal authentication or encryption. This creates a challenge because binary scans don't address many security weaknesses that can lead to a breach or breakdown, such as authentication and the insecure use of crypto.

What this means for security teams is that they must examine ALL files and identify suspicious indicators of compromises (IOC). Beyond that, they must also examine all build and container files for malware and occlusions, including packages and installers larger than 1GB.

Myth 3: You Can Trust Certificates and Code Signatures

Certificates and code signatures essentially verify that a piece of code or a web application is secure. This may sound good on paper, but when attackers gain access to an enterprise and a core build server, teams will find that certificates and code signatures are insecure or have been manipulated or compromised.

Another growing threat are fake certificates which can validate malicious code and even steal private keys. Security teams must regularly inspect all crypto certificates. This includes examining the corresponding chain of trust for reputation, validity, and signs of a compromise.

Myth 4: If it Was Malware-Free at One Point, It's Always Malware-Free

Today new types of malware are constantly emerging and to make matters worse, it's coming from trusted sources that make it increasingly more challenging for detection to keep up. Adding insult to injury, other types of malware, which have been in place for some time, can suddenly change disposition from an unknown state to bad. This is why patching has become a widely used practice in keeping machines updated and safe from threats.

Whichever form of malware you're dealing with, it often gets introduced as software versions are updated and after that it quickly blends with existing code. This is most common when working with open-source repositories, cloud containers, APIs, IoT, and extended supply chains which ultimately extend the scope of social engineering, including ransomware.

To fight back, teams must adopt a secure software development lifecycle (SDLC) approach that provides scanning and analysis at every stage of software deployment and use.

Mitigating Against Future Software Supply Chain Attacks

Calling out these misconceptions, ReversingLabs recognizes that security and software development teams need help. Businesses are under pressure to get software product releases out the door quickly and without any compromise on the quality. It's this pressure that causes steps to be missed and corners to be cut. To help improve the security of the software development supply chain we have introduced ReversingLabs Managed Software Assurance Service.

Built on the foundation of our Titanium Platform, the on-demand offering provides businesses with an advanced analysis that can examine in-house developed or third-party software packages for signs of tampering and malicious or unwanted additions, all before they are released to customers or across the enterprise.

Customers simply upload software packages requiring analysis via a secure channel to ReversingLabs. Once complete, the ReversingLabs team analyzes, interprets and provides guidance. Specific services provided include:

- Deep inspection for malware and post exploitation vulnerability presence through recursive package decomposition, extracting all possible components for advanced analysis.

- Software grading based on code signing process and application hardening using software vulnerability mitigation techniques.

- Analysis reporting that describes a full and validated software bill of materials, software quality metrics, malicious behavior and explainable insights tracked across software versions.

- An audit report in both machine-readable and human-readable formatting for all embedded files.

- Designated ReversingLabs research analyst to verify whether software is fit for its purpose and safe to put in production.

Once complete, our team analyzes and interprets the package and then provides developers with clear and accurate information on their builds. In the end, by analyzing the files for malware and highlighting the differences, our service can help prevent these attacks before the software is released to the end-users.

In an increasingly software driven world, the onus is squarely on companies to take the proper steps to mitigate supply chain threats. The process includes gaining greater awareness into best practices as well as access to new offerings such as our Managed Software Assurance Service. By leveraging best practices , teams can achieve the 100 percent confidence that the software they‘re sending out is malware free.

About the Author

Jasmine Noel is Senior Product Marketing Manager at ReversingLabs. Her career began as an industry analyst covering IT technologies. She then founded Ptak, Noel & Associates to provide research and marketing services to Fortune500 and startup technology firms. Prior to ReversingLabs, Noel also held product marketing roles in growth companies, including Veracode, Corvil and NS1. Jasmine can be reached Twitter at @ jnoel_work_life and at our company website http://www.reversinglabs.com

Secureworks® Interactive Adversary Software Coverage Tool Models Threats Against MITRE ATT&CK®

Easy-to-use free MITRE mapping tool puts the power of predictive attack modeling into defenders' hands

By Michael Rosen - Director of Technical Marketing

Increasingly sophisticated and widespread cybersecurity incidents have security practitioners clamoring for a better approach to breach detection and remediation. Threat actors are increasingly exploiting gaps in point solutions and vulnerabilities in the supply chain, highlighting the need for organizations to model their end-to-end attack surface, while struggling with limited security staff and disparate tools. This has increased the need to quickly evaluate and deploy security solutions best suited to the environment.

In a crowded space with vendors competing with each other instead of focusing on the common adversary, how can organizations cut through the noise to identify the best solutions for their needs?

The new **Adversary Software Coverage (ASC)** tool allows users to interactively explore how **Secureworks Taegis XDR** maps coverage and countermeasures to the tactics and techniques used by over 500 adversarial software types against the MITRE ATT&CK framework, including the latest ATT&CK v9.

With no prior exposure to XDR, users of all technical skill levels can quickly use the ASC tool to:

- **Model cyberattacks** by threat category or malware name in advance of breaches to harden defenses
- **Understand attack sequences** in terms of adversary software behaviors mapped to MITRE ATT&CK techniques
- **Visualize the end-to-end attack surface** and the security tools needed to minimize exposure and reduce risk

The tool previews granular XDR detection visibility against real threats mapped to MITRE ATT&CK—the common language adopted by the InfoSec community—showcasing the unique value of Taegis XDR to security practitioners and business leaders making the security procurement decisions. It previews the specific attack footprints of a wide variety of threat types and identifies key points in the attack chain where Taegis XDR offers deep actionable insights into breaches and streamlines incident response.

Secureworks makes transparent MITRE coverage accessible to everyone

The tool is open to the public freely and with no obligation. It is simple to use, highly interactive, and deeply granular in coverage mappings of the techniques and sub-techniques used by adversaries in their attacks. It's fully transparent, showing areas of "coverage" and "no coverage" aiming to increasing total attack surface visibility using multiple security controls—dozens of which are supported by XDR integration. This sets it apart from similar MITRE mapping tools that show visibility only in the most favorable light for the specific vendor producing the coverage map.

What MITRE alignment says about Taegis XDR

Taegis XDR defenses and countermeasures cover more than 90% of all adversarial TTPs tracked by MITRE, across all framework categories. Taegis XDR and Taegis ManagedXDR are built to detect threats that evade the layers of defensive security stacks, especially preventative layers like the Next-Generation Firewall or the Endpoint Protection Platform. Taegis XDR extends from endpoint to network to cloud, with sensors deployed at strategic locations across the enterprise to deliver maximum visibility. As a multi-vector detection technology, XDR sees these attacks from a comprehensive vantage point by combining the visibility from various single-purpose tools to increase total attack surface coverage.

How to use MITRE ATT&CK when considering security vendors

Mapping to the MITRE standard shows how security tools can positively impact detection capabilities and reduce attack surface blind spots in advance of an incident. Tools with strong MITRE mappings help organizations make informed security stack decisions, serving as a yardstick to source the fewest tools for the greatest amount of attack surface coverage. Placing controls onto MITRE maps help avoid coverage overlaps and gaps in an organization's cyber defenses and increases return on security investments.

No single tool or vendor can do it all

Be wary of vendors who claim 100% MITRE ATT&CK coverage—or even 100% across a single category of attacks—ransomware, trojans, botnets, etc.—as the adversarial tactics, techniques and procedures are constantly evolving, and the list of malicious software continues to grow. When evaluating vendors, be sure to ask about their capabilities and their limitations. Use MITRE to validate which products fill key visibility gaps for the organization's primary security use cases to get as close as possible to a comprehensive attack surface coverage with minimal repetition across tools. Be sure vendors can substantiate claims at a granular level by asking to see the corresponding detections within their tools.

Please take a test run of the **Taegis XDR ASC tool** and explore the adversarial behavior that Taegis XDR sees across a library of hundreds of real-world malicious software tools.

About the Author

Michael Rosen - Director of Technical Marketing

Michael Rosen is Director of Technical Marketing for Secureworks. He has a decade of hands-on cybersecurity background in endpoint, network, datacenter and cloud security technologies, and 25 years of overall secure technology experience including a variety of technical and product-related roles. Michael has spent half his career as a product manager and half as a product marketer. He has an MBA in Information Systems and a JD in Law. He lives in San Diego, California with his wife of 24 years and has two college-aged children.

About This Publication

The Black Unicorn Report is a once-per-year publication of the Cyber Defense Awards and Cyber Defense Magazine team, two leading platforms of the Cyber Defense Media Group.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

www.cyberdefenseawards.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)
Cyber Defense Magazine – Black Unicorn Report rev. date: 08/02/2021

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

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

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

THE BLACK UNICORN REPORT

With David DeWalt, Robert Ackerman and Gary Miliefsky

and our newest judge, this year: Dr. Peter Stephenson

www.cyberdefenseawards.com