SECURITY FIRST

Cyber Security Conference 2022

LONDON

April 28th, 2022

IET London: Savoy Place

www.securityfirst2022.co.uk

DUBLIN

MAY 11th, 2022

Aviva Stadium Dublin

www.securityfirst2022.ie

Integrity360

your security in mind

Foreword

I am delighted to welcome you to the 2022 Security First conference hosted by Integrity360.

Every day, our team speaks to cyber security and IT professionals from across all industries who find themselves having to operate in very challenging environments that are growing in complexity each and every week. The biggest challenge of all is having to operate and defend yourselves from an invisible enemy, from attackers and criminals that operate from the shadows and who are working relentlessly and ruthlessly to be 2 steps ahead of you.

It is why we at Integrity360 embrace the ethos of "putting Security First". The digital world in which we all operate relies on 24 hours a day, 7 days a week and 365 days a year functionality that IT professionals such as you are tasked with maintaining. Putting Security First is the only way to operate these IT environments safely, reliably and constantly. It is also the right way to invest in any migration, evaluation or synchronisation of digital infrastructure.

It is also why we run these conferences to bring together cyber security and IT professionals like you to hear about the latest trends, technologies and strategies that can hopefully help you stay that step ahead.

We encourage you to attend our keynote sessions, ask questions of our panelists, network with your peers and others from the industry and hopefully take away actionable insights to bring back to your business about how you can improve you own strategy, processes, and systems to foster a better security posture.

Thank you once again for joining us and please come over to say hello if you see me throughout the day.

Ian Brown
Executive Chairman, Integrity360

It takes 20 years to build a reputation and a few minutes of a cyber incident to ruin it

"Failing to prepare is preparing to fail" – Benjamin Franklin

Sponsors

Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Rather than offering a static one-size fits all approach that stifles innovation and creates vulnerabilities, Forcepoint solutions inherently understand how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

FORCEPOINT.COM

CHECK POINT™

Check Point is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from 5th generation cyber-attacks with an industry-leading catch rate of malware, ransomware and other types of attacks. Check Point offers multilevel Security Architecture, "Infinity" Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system.

CHECKPOINT.COM

VARONIS

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects cyberthreats from both internal and external actors by analysing data, account activity and user behaviour; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. Varonis started operations in 2005 and has customers in major leading firms from various industries.

VARONIS.COM

splunk>

Splunk is the data platform leader for security and observability. Our extensible data platform powers enterprise observability, unified security and limitless custom applications. Splunk helps tens of thousands of organizations turn data into doing so they can unlock innovation, enhance security and drive resilience.

SPLUNK.COM

Sponsors

FORTINET

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 565,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs

FORTINET.COM

VECTRA

Vectra® is a leader in threat detection and response for hybrid and multi-cloud enterprises. The Vectra platform uses AI to detect threats at speed across public cloud, identity, SaaS applications, and data centres. Only Vectra optimises AI to detect attacker methods—the TTPs at the heart of all attacks—rather than simplistically alerting on "different". The resulting high-fidelity threat signal and clear context enables security teams to respond to threats sooner and to stop attacks in progress faster. Organisations worldwide rely on Vectra for resilience in the face of dangerous cyber threats and to prevent ransomware, supply chain compromise, identity takeovers, and other cyberattacks from impacting their businesses. For more information, visit vectra.ai.

VECTRA.AI

RAPID7

Rapid7 simplifies cybersecurity. With powerful automation and integrated threat intelligence from our industry-leading researchers and SOC analysts, our Insight Platform gives security teams the visibility they need to secure their environment no matter the size or complexity. Don't just protect your business, drive it forward.

RAPID7.COM

Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers. More at https://trellix.com

TRELLIX.COM

Sponsors

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose-built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack—providing complete, multi-layered protection against threats across hybrid environments. For more information, visit www.deepinstinct.com and follow us on LinkedIn and Twitter.

DEEPINSTINCT.COM

The average company is mentioned 15 million times a year. Finding the risks within this vast amount of data is a considerable challenge. Digital Shadows help you filter out the noise, automate your response, and focus analyst time on addressing the digital threats most critical to your organization. Digital Shadows SearchLight allows your team to take the right action faster. To learn more visit www.digitalshadows.com.

DIGITALSHADOWS.COM

Mimecast are the company that built an intentional and scalable platform that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world.

MIMECAST.COM

F5 helps organizations deliver and secure extraordinary digital experiences. Through a portfolio of automation, security, performance, and insight solutions, F5 empowers customers to create, secure, and operate adaptive applications. These applications will naturally adapt based on their environment—growing, shrinking, defending, and healing themselves—so organizations can focus on their core business, increase revenue, improve operations, and build trust with their customers.

F5.COM

Sponsors

XM Cyber

XM Cyber is a hybrid cloud security company that's changing the way innovative organizations approach cyber risk. Its attack path management platform continuously uncovers hidden attack paths to businesses' critical assets, enabling security teams to cut them off at key junctures and eradicate risk with a fraction of the effort.

XMCYBER.COM

Qualys.

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide. The Qualys Cloud Platform and its integrated security solutions continuously deliver critical security intelligence to businesses across their lobal IT assets.

QUALYS.COM

Cynet

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

CYNET.COM

The World's Fastest Firewalls

CHECK POINT
QUANTUM LIGHTSPEED

For The Most Demanding Datacenters and e-commerce

Introducing Quantum Lightspeed Firewalls. Check Point's Quantum network security family has expanded with the addition of six new hyper-fast firewalls, delivering 200 Gbps to 800 Gbps of firewall throughput. Experience security at the speed of your network, with ultra-low 3 µSec latency for the most sensitive applications.

And when integrated with Quantum Maestro, easily scale your security to 3 Tbps throughput, with industry leading High Availability using Check Point's patented HyperSync, N+1 Active-Active failover architecture. Maestro also automatically load balances traffic across your firewall array – for the highest rated network security and best price-performance in the industry.

YOU DESERVE THE BEST SECURITY

CHECK POINT™

checkpoint.com/quantum/

CHECK POINT™

From SolarWinds to Log4j: The global impact of today's cybersecurity vulnerabilities

If the past year has taught businesses anything, it's that the impact of targeted cyberattacks and security vulnerabilities is now, without doubt, universal. From the fallout of the SolarWinds software supply-chain attack to the exposed Apache Log4j vulnerability, the case for organizations of all shapes and sizes to have a comprehensive and robust security infrastructure in place has never been stronger, even if they themselves aren't necessarily in the cross-hairs.

Many regard the now-infamous SolarWinds breach in late 2020 as a major catalyst for what would become a frenzy of "Gen V" or fifth-generation attacks that persist to this day. Such large-scale, multi-vector attacks have virtually unlimited reach, with devastating security consequences for businesses and governments around the world. A year later, the Apache Log4j vulnerability was exposed, which made it possible for malicious actors to execute code remotely on almost any targeted computer to take control, steal data or even hijack a user's machine to mine cryptocurrency.

The former was an orchestrated attack by an advanced persistent threat group, the latter was an exposed zero-day vulnerability that nobody saw coming. One thing both incidents have in common, however, was that they increased risk and vulnerability for businesses in every sector, in every corner of the world. As organizations plot their course through 2022 and beyond, it's never been clearer that cybersecurity is a global issue rather than a local one, and this should be reflected in every cybersecurity strategy moving forward.

The rise of "Gen V" attacks

Gen V attacks are unique in the way that they leverage broad attack surfaces and multiple infection vectors to infiltrate large numbers of organizations, and they are increasing at an unprecedented rate. At a time when businesses and government agencies are expanding their network footprint, adding more endpoints and connected devices into their technology mix, the risk of being impacted by a Gen V attack has also never been higher. As outlined in our 2022 Security Report, the SolarWinds breach, which impacted more than 18,000 organizations around the world, kickstarted a torrent of supply-chain attacks that still plague businesses today. In a year that saw cyberattacks against corporate networks increase by 50% across the board, software vendors like SolarWinds experienced the largest year-on-year growth in attacks with an increase of 146%. Today's corporate economy is built on an intricate web of software supply chains, which means that with every additional attack on a software vendor, the vulnerability of businesses around the world is further amplified.

From SolarWinds to Log4j: The global impact of today's cybersecurity vulnerabilities

Fueling attacks: the Sunburst catalyst

The SolarWinds software supply-chain attack was facilitated by a back door known as 'Sunburst', which was added to the SolarWinds Orion system before being distributed to customers globally via a routine update. This gave the APT (advanced persistent threat) group involved covert access to thousands of SolarWinds customers' networks, from government agencies to Fortune 500 companies. Unfortunately, this mode of attack from APT groups is now on the rise. As our report details, the REvil ransomware group targeted multiple managed service providers (MSPs) throughout 2021, and in July managed to embed a malicious software update in IT company Kaseya's patch management and client monitoring tool. Thousands of unsuspecting businesses were impacted, with millions of US dollars demanded in ransom.

Sunburst also likely inspired the attack on Colonial Pipeline, which carries almost half of the fuel consumed by the US East Coast. The nation-state APT group, DarkSide, was allegedly behind the attack, employing a Ransomware-as-a-Service model, meaning it relied on third-party affiliate programs to orchestrate the breach. This is one of the most striking examples to date of how tools used to carry out such attacks are becoming democratized and more widely used, again ramping up the pressure on businesses to guard their perimeters.

While the assets of the REvil ransomware group have since been seized and its ringleaders arrested, you cannot arrest code. Once one threat group makes headway with a particular attack, it doesn't take much for an affiliate member to keep that momentum going. Emotet, one of the most dangerous botnets in history, made a return in November 2021 following its take-down a year earlier. It's a trojan primarily spread through links, spam emails, malicious scripts and macro-enabled document files, and once it infects a user it can spread like wildfire without detection, stealing banking credentials and financial data from individuals, companies and governments around the world.

Ambushed by zero-day vulnerabilities

While targeted attacks like the ones outlined above are presenting an increased threat to organizations around the world, so are exploits and vulnerabilities. In December last year, a remote code execution vulnerability was reported in Apache Log4j, the most popular java logging library in the world. This library is embedded in almost all of the services and applications we use in our day-to-day lives, from

From SolarWinds to Log4j: The global impact of today's cybersecurity vulnerabilities

Twitter and Amazon to Microsoft and Minecraft. Initially used by some threat actors to leverage cryptocurrency mining resources at the expense of their victims, there's no reason an exploit like this couldn't be used for more sophisticated and nefarious attacks. Check Point Research detected approximately 40,000 attack attempts just 2 hours after the Log4j vulnerability was revealed, and a further 830,000 attack attempts 72 hours into the event.

These zero-day vulnerabilities earn their name from their ability to completely blindside businesses, giving them virtually no time to react before they become potential victims. It then becomes a race between threat actors and their ability to exploit the vulnerability, and how quickly businesses can close the gap in their defenses.

Global threats require a global solution

The threat climate has changed. The traditional defensive line that businesses can draw between themselves and the rest of the cyber landscape has become blurred to the point that it may as well not exist. Instead of guarding a static perimeter, businesses need to take a more holistic and real-time view of their security infrastructure. Security practitioners need to be able to maintain 360-degree visibility of their entire network, regardless of how far and wide it has been distributed. They also need access to real-time threat intelligence on a global scale, so they can pre-empt far-reaching zero-day vulnerabilities and targeted software supply-chain attacks like the ones outlined above.

Check Point's Infinity platform, for instance, is the only security platform of its kind that offered pre-emptive protection for customers against the Log4j exploit. It's the first modern, consolidated security platform specifically designed to guard against zero-day vulnerabilities and sophisticated fifth-generation attacks across all networks, cloud deployments and endpoints. Part of Infinity's success is its ability to leverage Check Point's ThreatCloud, a real-time global threat intelligence platform that monitors networks around the world for emerging threats and vulnerabilities.

If organizations around the world want to operate safely and securely in 2022 and beyond, they need to start seeing cybersecurity as a global issue rather than a local one, and evolve their security strategies accordingly. Only then will they be able to confidently defend themselves against a threat landscape that knows no bounds and cannot be contained by borders.

Find out more: **www.checkpoint.com**

How Digital Shadows Works for You

IDENTIFY THE REAL THREATS. MAKE DECISIONS FASTER_

Expertise Meets Data

ACCESS

Digital Shadows provides access to the widest range of data sources and the expertise needed to turn that data into intelligence.

Identify What's Important

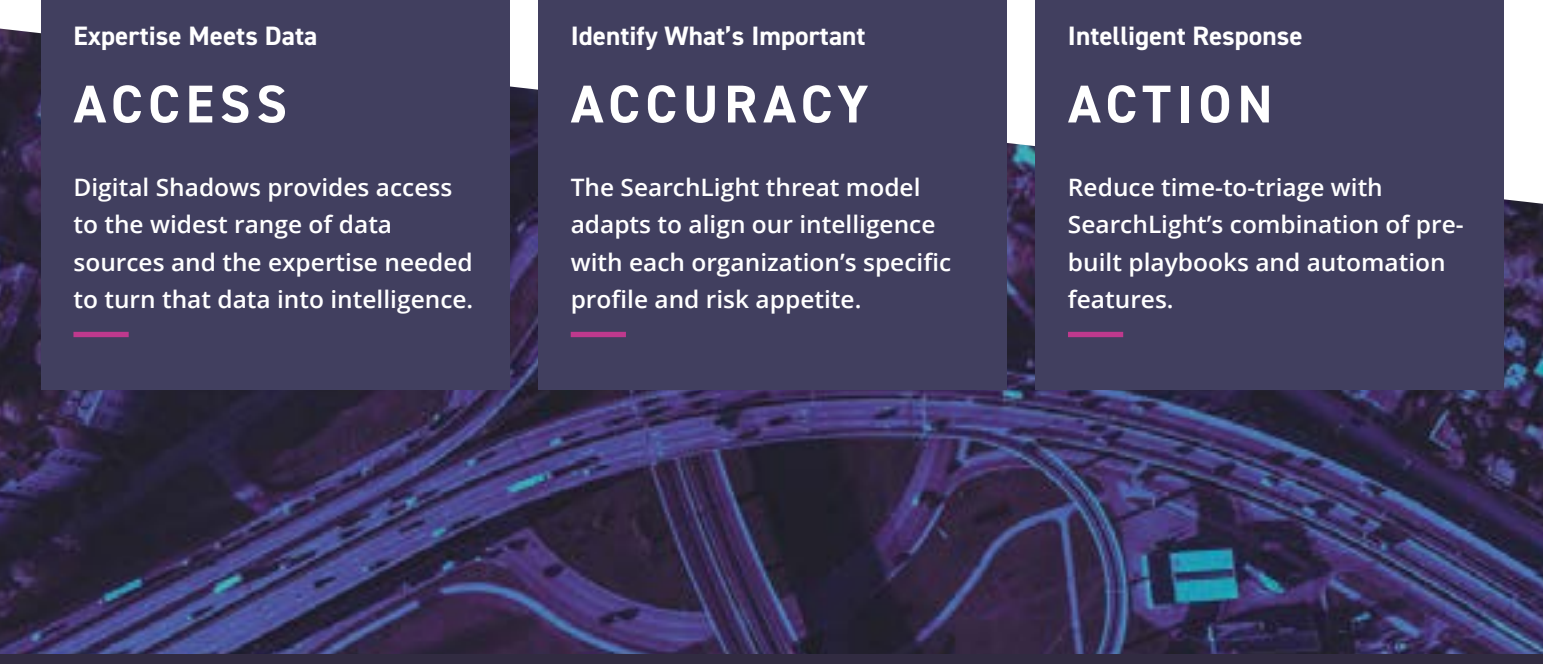
ACCURACY

The SearchLight threat model adapts to align our intelligence with each organization's specific profile and risk appetite.

Intelligent Response

ACTION

Reduce time-to-triage with SearchLight's combination of pre-built playbooks and automation features.



SEARCHLIGHT

ACTIONABLE THREAT INTELLIGENCE FOR YOUR SECURITY TEAM

SearchLight provides actionable threat intelligence that adapts to your organization's specific risk profile and appetite. By combining advanced data analytics, API integrations, and automation features, SearchLight allows your team to take the right action faster.

Learn more or get a free trial at www.digitalshadows.com

digital shadows_

The Need for a Zero Trust Edge Strategy

John Maddison

Today's hybrid workers require access to distributed applications deployed in the datacenter, multi-cloud environments, and SaaS locations. Digital acceleration involves adopting and implementing new technologies and practices to improve business agility and employee productivity. But it is also redefining the network edge—especially in today's Work-from-Anywhere world where users move between on-premises locations, interconnected branch locations, home offices, and temporary locations during travel—thereby expanding the attack surface and exposing the business to new, advanced threats.

Unfortunately, most traditional network architectures were built using disparate and statically deployed point products that provide implicit access to all applications. However, such an approach is no longer effective at providing secure access to critical resources at scale, especially as users, devices, and applications are in constant motion. And the inevitable rerouting of traffic to fixed security points for inspection severely impacts user experience, especially when those tools cannot adequately examine encrypted application, data, and video streams. Far too often, the default response in many organizations has been to bypass security to not impact critical business operations. And the result has been disastrous, with ransomware, phishing, botnet, and other criminal activity now at an all-time high.

What's needed is a secure Digital Acceleration strategy that ensures that new technologies can be adopted and new, highly dynamic edges can be established without compromising the protection of critical data or the security of users and devices. Zero-trust is based on the principle that every device or user is potentially compromised, and therefore every access request must be authorized and continuously verify. And even then, users and devices can only access those resources required to do their job and nothing more.

This same approach is now being applied to the remote edges of the network, a strategy known as the "Zero Trust Edge." This new zero-trust approach to securing the expanding edges of today's networks helps ensure that Security-Driven Networking – the critical convergence of security and networking – is everywhere. This enables security to seamlessly adapt to dynamic changes to the underlying network infrastructure, including connectivity, while providing explicit access to applications based on user identity and context.

Security-Driven Networking from Fortinet

Forrester recently described a solution they have dubbed the "All-In-One Zero Trust Edge" in the Now Tech Report published in December 2021. In that report, they described the future of next-generation networking infrastructure as bringing together networking and security in any combination of cloud, software, and hardware components, securely interweaving users, data, and resources using essential zero-trust principles.

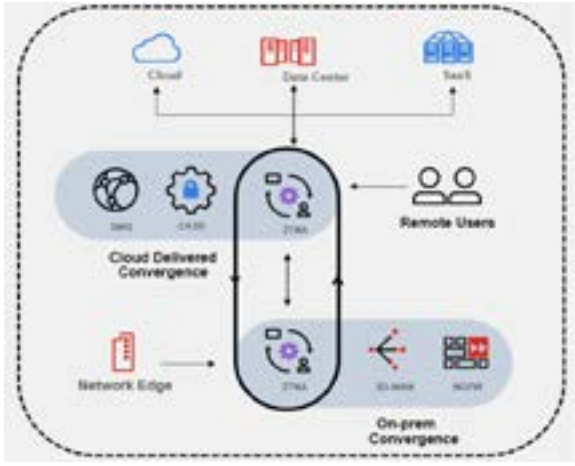
Fortinet is recognized in this report. We believe that's because we uniquely bring together all components needed to converge networking and security and can then deploy them on

The Need for a Zero Trust Edge Strategy

John Maddison

premises and in the cloud, including SD-WAN, NGFW and ZTNA. This ensures that we can deliver consistent convergence and zero implicit trust everywhere. We call this Security-Driven Networking.

Fortinet's Security-Driven Networking approach starts with FortiOS-based innovations, including our on-premises SD-WAN and next-generation firewall secure access solutions, which also includes built-in ZTNA. It continues in the cloud with Fortinet's cloud-based secure web gateway, CASB, and ZTNA solutions for remote users.



What is a Zero Trust Edge Solution?

Fortinet's Security-Driven Networking innovations deliver the industry's most complete Zero Trust Edge solution:

1. SD-WAN: Providing better path and user-experience to applications and services using SD-WAN is foundational for Trust Edge solution. Fortinet was the first vendor to blend advanced security and connectivity into a unified solution. Our Secure SD-WAN solution securely interconnects all offices to every datacenter, multi-cloud, and SaaS environment. And in addition to reliable connectivity and cloud on-ramp, it includes a full suite of advanced security, enables dynamic segmentation to prevent lateral threat movement for East-West protection, and maintains superior user experience through digital experience monitoring.

2. Hybrid Convergence of Networking and Security: Zero Trust Edge must also support today's highly dynamic networks. Legacy security solutions struggle to provide consistent policy distribution, orchestration, and enforcement when the underlying network is in constant motion. Integrating security and networking into a unified system is essential for deploying consistent security everywhere, both for on-premises and remote users. Fortinet is the only vendor to deliver networking and security convergence powered by the same operating system (FortiOS) to offer seamless policy distribution and orchestration. We also provide the industry's highest security performance using our purpose-built security ASICs, enabling the inspection of encrypted traffic, including streaming video, without impacting user experience.

The Need for a Zero Trust Edge Strategy

John Maddison

3. Secure Remote Access: Cloud-delivered security that securely connects all remote users is essential to any Zero Trust Edge solution. Comprehensive web security from the cloud must provide multiple layers of defense with AI-driven web filtering, video filtering, DNS filtering, IP Reputation, Anti-botnet service including the ability to address data loss prevention and protect mobile users with in-line CASB integration.

4. ZTNA Everywhere: Finally, Zero Trust Network Access (ZTNA) is essential for securing access to the critical applications and resources today's hybrid workforce demands. However, protecting a hybrid workforce that may be in the office one day, working from home the next, and traveling another requires a ZTNA solution that is available everywhere users or devices are located. Unlike traditional VPN, ZTNA provides explicit access to users per application based on identity and context. Fortinet is the only vendor with a ZTNA solution designed to protect access from any edge, not just a few edges.

Fortinet's Security-driven Networking Approach to Zero Trust Edge

Fortinet's innovative approach to Zero Trust Edge converges enterprise-class security and networking everywhere across the network. This unique ability ensures secure access to critical applications and resources, whether users are on-premises or accessing resources through the cloud. Our Security-Driven Networking approach—including our unique combination of exclusive purpose-built ASICs, cloud-delivered security solutions, and integrated networking capabilities—enables superior user experience combined with coordinated threat protection for every network edge.

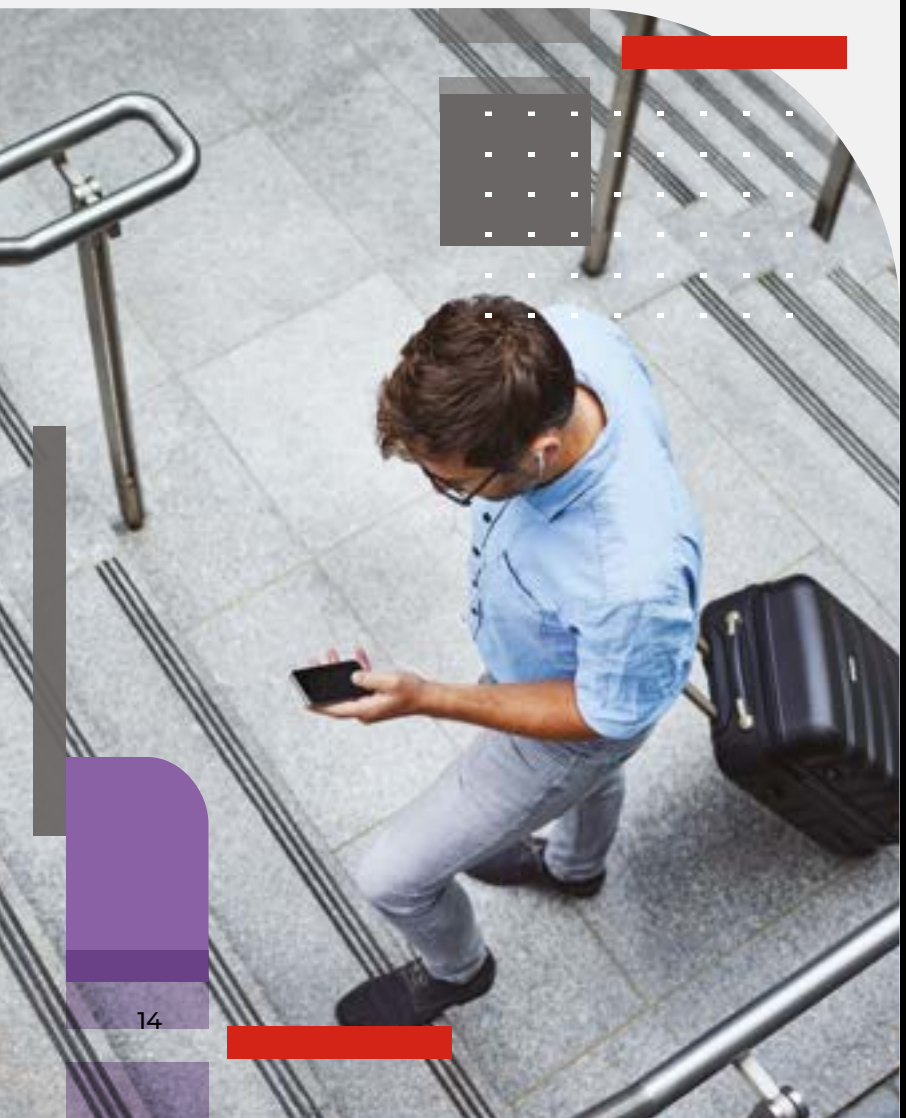
Zero Trust Edge resolves one of the most enduring challenges facing today's IT teams: extending enterprise-grade security and granular access control to remote workers. Fortinet's Security-Driven Networking approach provides a unique solution to overcoming user experience, siloed and disconnected networking/security technologies, and implicit trust challenges that create obstacles for today's organizations serious about digital acceleration and implementing an effective—and secure—work from anywhere strategy.
Read more about Zero Trust Edge in the recent Forrester report and find out how you can implement an enterprise-wide Zero Trust Edge architecture with Fortinet's Security-driven Networking approach. **www.fortinet.com**

FORTINET®

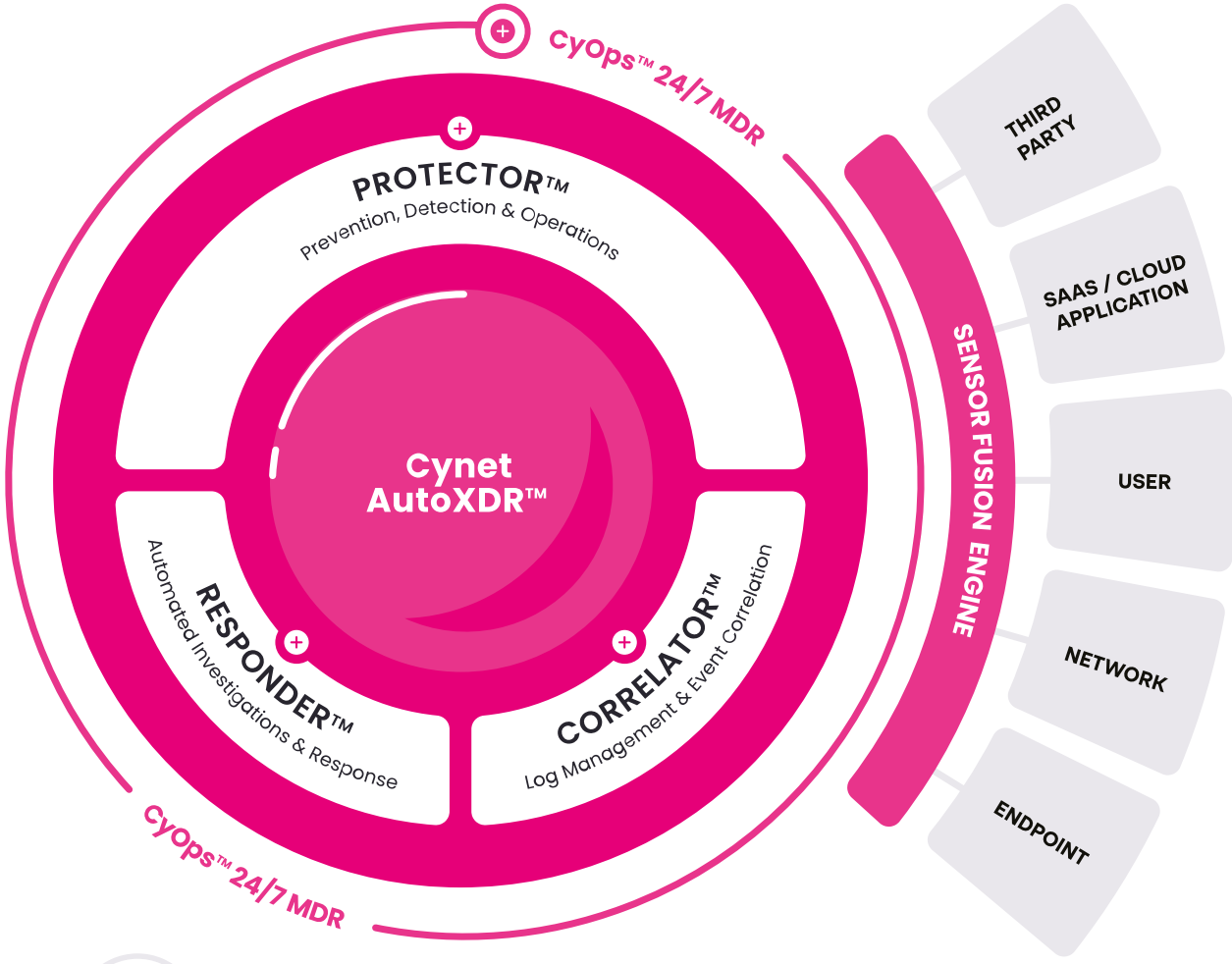
Zero Trust Access
Keeping control over who and what can access the network

Digital Security,
everywhere you need it

fortinet.com



Cynet enables any organisation to put its cybersecurity on **autopilot** by natively consolidating the essential security technologies needed to provide comprehensive threat protection into an **easy-to-use XDR platform**, automating investigation and remediation across the environment, and providing a **24/7 proactive MDR service** - at no additional cost.



Download a free 14 day trial

Integrity360

your **security** in mind

Calm within the chaos

Having an expert team of cyber security specialists ready to respond when you need it most can be critical for maintaining composure un the midst of the chaos than an incident can bring.

Find out more about our Incident Response Services

www.integrity360.com/incident-response

Forcepoint

SASE Security and the new Security Service Edge (SSE)

Jim Fulton, VP Product Marketing & Analyst Relations, Forcepoint

Today the internet is a hostile threat landscape where many of its users and devices operate on unmanaged networks. In addition, many businesses store their resources in the cloud, which is populated by more users, applications, and devices than ever before.

Despite the need for the right digital protection measures, security teams have been slow to react to the current threat landscape due to complexity, product sprawl and rising costs.

To address these issues, over the last two years we've seen a new class of integrated, cloud security solutions emerge, dubbed "Secure Access Service Edge" or SASE (pronounced "sassy"). SASE brings together networking and security to enable secure connectivity that is delivered consistently wherever people were working. Due to the rapid adoption of this approach, last year Gartner coined the term "Security Service Edge" (SSE), an easy way to carve out the security elements of SASE.

What is SASE Security or SSE?

Whether you call it SASE security or SSE, this unified approach to providing security as a service for employees no matter where they are working, enables security policies to be defined, monitored and enforced in one place. It protects people as they use business applications and data, whether that's through: the web, cloud apps like Microsoft 365, or private applications in internal data centers or private clouds and gateways such as a Cloud Access Security Broker (CASB), Secure Web Gateways (SWG) or Zero Trust Network Access (ZTNA).

Why does your business need SASE and SSE?

SASE and SSE improve operations and security in several ways:

1. It provides consistent security on work-issued and personal devices for users anytime, anywhere.
2. It offers all-in-one management and delivery of crucial security features, such as anti-malware, URL filtering, and both on-site and cloud protection.
3. It eliminates the need for multiple vendor subscriptions, miscellaneous security equipment, and provides a complete security solution. This also reduces costs.
4. SASE provides security from a centralized position, which allows for better, more efficient performance, especially for interactive cloud apps like Microsoft 365.
5. Cloud-based security can rapidly scale up and down to meet changing needs.

Unified, cloud-delivered security provides the robust, consistent security everywhere for organisations without sacrificing efficiency or putting sensitive data at risk. With the return to the office post-pandemic creating new challenges for the security team, now is the time for businesses to look towards SASE security and SSE solutions.

www.forcepoint.com

Forcepoint

Security Finally Has an Easy Button

Manny Rivelo, Chief Executive Officer, Forcepoint

Today we have more bandwidth and digital innovation than ever, which creates risk and complexity. With 75% of employees are working remotely, more mobile device connections than people on the planet, and the average enterprise managing 288 different SaaS apps, it's perhaps no surprise that security teams are struggling.

With the average CISO managing 50 or more products, having visibility of all of this is near impossible. Yet it's expected every day. No wonder there is a cyber talent shortage, while the cost of cyber crime has grown to more than $6 trillion annually.

In recent years security has become a mixture of capabilities and features, and teams are chasing after different combinations of letters trying to prevent risk. If employees connect to a website, a Secure Web Gateway (SWG) is needed to block them from accessing high-risk sites or download malware or upload sensitive data. If teams connect to a cloud SaaS app, a Cloud Access Security Broker (CASB) is required. And if individuals are trying to access a private app like an ERP, a Zero Trust Network Access (ZTNA) is vital.

The old architecture to support this required a perimeter, yet we know this has dissolved and now involves employees working on a mix of company and personal mobile devices in the office or anywhere with a Wi-Fi connection. This is flawed and needs to change.

It's time to simplify. Simplifying security doesn't mean getting rid of or reducing capabilities. We still need a SWG or a CASB or ZTNA. But why do we have to treat accessing the web, the cloud, and private apps as silos? We can simplify by unifying technologies into a single platform, providing just one management console to manage one set of security policies, and one unified endpoint agent.

Forcepoint has taken a huge step to simplify security with the launch of Forcepoint ONE. Forcepoint ONE makes it easier for businesses to implement Zero Trust with certainty, to stop ransomware and other malware in their tracks, to know your data is safe wherever you need it.

As Steve Jobs said, "Simplicity is the ultimate sophistication." To simplify anything is hard. After all, it's been too easy for our industry to build out a conga line of products. Security has gotten too complicated, and it doesn't need to be. Security should be simple to use and manage. Finally, security has an easy button.

Forcepoint

5 Steps To Vendor Consolidation

Ed Stirzaker, VP Northern EMEA at Forcepoint

The modern IT team is inundated with tools and software. Almost 80% of CISOs have 16 or more cybersecurity tools in their portfolio, according to Gartner's 2020 CISO Effectiveness Survey. Staggeringly, 12% have 46 or more. With this many pieces of software in operation, it's no surprise that vendor consolidation was one of the top security and risk trends of the year in 2021.

Removing vendor bloat

Vendor consolidation is all about businesses reducing the number of vendors they work with down to a small group of companies. Consolidation can cut costs, streamline operations and reduce organisational blind spots.

While the cost savings can be very compelling, that alone doesn't solve all the problems. There's also the pressure of tightening budgets, more streamlined teams, and the reality of cybercrime today – that is ever-more frequent and damaging to organisations that are more digitally-driven and remotely run than ever. Ongoing economic uncertainty, not just from the pandemic but also wider global events, are also seeing organisations cut back where they can.

Security tool trade-offs

Simply letting go of tools and vendors is difficult in practice. It can be hard to know what to look for, and how to evaluate what's genuinely needed and what can be safely stopped. There are five key steps to getting this right:

1. The first step is to gauging the size of the problem by auditing what tools and services teams are currently using.
2. Next comes finding out why these tools ended up in place. What value are they bringing?
3. Then comes working out where there's potential overlap. Good vendors will be those who are willing to be a strategic partner, help with your consolidation and cost goals so the business can achieve its goals.
4. After this comes the honest conversations with your vendors on what goals you're trying to reach, and how best to work together in the future.
5. Finally, keep the conversation going. Hold vendors to account and review the delivery and support models that have been built to make you're your objectives are being met with the tools that are in place.

All businesses want to reduce the number of suppliers they're using if they can. If they get it right, there are huge efficiency gains to be made. In a world where all-in-one cloud security platforms are becoming the norm, now's the time to review and consolidate.

Integrity360

your **security** in mind

Managed Detection & Response

Preventative measures alone are not sufficient

MDR combines & integrates industry leading Threat Detection & Response tools with unparalleded security expertise scale & leadership to proactively protect you from Internal & External threats.

Find out more about our Managed Detection & Response Services

www.integrity360.com/managed-security

Defending Your Cloud Environment Against LAPSUS$-style Threats

The LAPSUS$ cybercrime group made headlines recently after taking credit for high-profile attacks on major companies including Microsoft, Okta, Samsung, Ubisoft, and NVIDIA (confirmed by Microsoft and Okta). This group's goal, like many others, is to steal sensitive data, threaten to leak it, and extort their victims.

U.K. police arrested seven people, between the ages of 16 and 21, as part of an investigation into the LAPSUS$ group.

Methods of Operation

Unlike your standard ransomware groups that deploy malicious payloads to mass encrypt and exfiltrate data, the LAPSUS$ group uses simple yet effective social-engineering techniques to infiltrate environments and steal sensitive data.

According to Microsoft:
"Their tactics include phone-based social engineering; SIM-swapping to facilitate account takeover; accessing personal email accounts of employees at target organizations; paying employees, suppliers, or business partners of target organizations for access to credentials and multifactor authentication (MFA) approval; and intruding in the ongoing crisis-communication calls of their targets."

In addition to these social engineering methods, LAPSUS$ employs tools to crawl public code repositories that identify exposed credentials or open RDP ports, as well as "redline" password-stealing software that gets them directly from the user.

Once they steal credentials and bypass MFA, they infiltrate your private network and public SaaS applications to begin searching for sensitive data. As a part of their attack path, they head to private GitHub repositories and collaboration platforms like Google Drive and Microsoft 365 to find additional credentials (preferably privileged users and admins) to escalate their privileges and expand their reach.

Rather than encrypting data before exfiltration, they directly download the data through a VPN or virtual machine. After which, they attempt to destroy the organization's original copies of the data, leaving no choice but to pay to get their data back or risk the hackers selling or leaking it online.

Intrusion Timeline

Security researcher Bill Demirkapi obtained a copy of the Mandiant investigation report with a detailed timeline of the techniques used in a recent LAPSUS$ intrusion.

Intrusion Timeline

Table 1 lists the major dates, associated events, and the applicable attack phase for the intrusion. All timestamps in this report are in Coordinated Universal Time (UTC), unless otherwise noted. For a detailed description of each attack phase, refer to **Appendix A: Targeted Attack Lifecycle.**

Date (UTC)	Event	Attack Phase
2022-01-16 00:33:23	First logon event from [SYSTEM NAME REDACTED]. Logon to [SYSTEM NAME REDACTED] from [SYSTEM NAME REDACTED] (10.112.132.64)	Initial Compromise
2022-01-19 19:19:47	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Initial Compromise
2022-01-19 19:45:39	Bing search for Privilege escalation tools on Github by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-19 19:47:58	UserProfileSvcExp.exe downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:31:19	Account [ACCOUNT NAME REDACTED] created on [SYSTEM NAME REDACTED]	Maintain Presence
2022-01-20 18:32:32	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Move Laterally
2022-01-20 18:39:43	Bing search for Process Explorer by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:40:04	Process Explorer executed by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:43:51	Bing search for Process Hacker by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:01	Process Hacker downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:17	Process Hacker execution by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:46:22	FireEye Endpoint Agent service terminated on [SYSTEM NAME REDACTED]	Establish Foothold
2022-01-20 18:46:55	Bing search for Mimikatz by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:48:24	Mimikatz downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:50:10	Mimikatz executed by [ACCOUNT NAME REDACTED] on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:55:29	C:\Windows\System32\sam.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:56:41	C:\sam.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges

LAPSUS$ showed a lack of OPSEC sophistication post-intrusion—searching Bing and Google from the victim's machine for off-the-shelf hacking tools and downloading them directly from GitHub.

According to Mandiant's report, they used ProcessHacker, Process Explorer, and Mimikatz to perform recon, establish a foothold, disable FireEye's endpoint agent, and escalate privileges.

The attackers compromised a user's Microsoft 365 account and began searching for sensitive files. They found an Excel file named **DomAdmins-LastPass.xlsx** in a shared location. The file presumably contained clear-text admin credentials, allowing the attacker to create additional accounts, add the accounts to a group called "tenant administrators," and setup email auto-forwarding rules to BCC email sent to sykes.com inboxes outside of the organization.

VARONIS

Detecting and mitigating SSO, IAM, and SaaS attacks

LAPSUS$ style threats can be hard, if not impossible to detect with traditional perimeter and endpoint security alone. They spend very little time on the endpoint before pivoting to cloud applications with stolen credentials or cookies.

The defender's job can be difficult when there aren't specific hashes, registry keys, and other static IOCs to trigger alerts. We recommend treating LAPSUS$-style attacks like you would treat an insider threat. Assume breach of the perimeter, limit access, and watch for abnormal deviations from baseline behavior.

Right-size access and reduce exposure

The end goal of most cyberattacks is to steal or encrypt valuable data. Knowing who has access to which data and remediating overexposure is key to reducing your blast radius. In the event a single account is compromised, you want to ensure the attacker must get elevated access to do meaningful damage.

Right-sizing access starts with permissions visibility. The low-hanging fruit is to inventory your super admins across your different cloud apps. Depending on the app, determining who has privileged access can be difficult. For example, in Salesforce you can create a custom user profile that mimics an admin account but is named something innocuous like "Sales Users."

Varonis identifies all of the privileged entities in your cloud environment

You should have policies setup to alert you when a user is added to a privilege group or given super admin privileges. In most organizations, this action should be extremely rare, so the alerts have high fidelity.

Another way to drastically reduce risk is to proactively identify where sensitive data is exposed publicly, to guest users (like contractors), or to all users in your organization. Limiting sensitive data that is accessible to large swaths of users will make it more difficult for groups like LAPSUS$--who often use credentials found in publicly exposed GitHub repositories or pay contractors for access--to find data worth stealing.

When you can pinpoint a user's entitlements quickly across multiple SaaS apps and data stores, answering "What could this person possibly have accessed?" can make investigation, response, and disclosure faster and more conclusive.

On multiple occasions, LAPSUS$ gained access to an employee's virtual desktop where the user was already logged into multiple SaaS applications like GitHub and Jira. Since a person can be represented by multiple user accounts in a multi-cloud environment, it's essential to be able to link these identities automatically so you can assess the potential access and easily aggregate the log events from that person.

Monitor user behavior across different apps and systems

Monitoring endpoints and identifying potential perimeter breaches is a must for any organization, but what happens when attackers bypass your endpoints altogether?

Analyzing user behavior and data activity is one of the best ways to identify a threat actor impersonating one of your users and stop them before it's too late.

Even if a group like LAPSUS$ performs significant research and reconnaissance on the user they've compromised, they still cannot perfectly mimic their behavior, especially as they move through your environments accessing and downloading large amounts of data.

It's essential to baseline behavior across all your users and all your critical apps and data:

- Profile which files/folders they typically use across M365, Box, Google, etc.
- Profile which websites/apps they connect to (Slack, Zoom) and what they typically do inside them
- Profile the devices/IPs/geos they use to connect to the VPN/cloud apps
- Profile AD/IdP/IAM activity--logins, permissions changes, password resets

Once you have rich peace-time profiles, sophisticated machine learning algorithms can detect even subtle deviations that could indicate compromised or malicious insiders.

LAPSUS$ is a prime example – they may have your credentials, phone number, recovery email, and IP address, but they still can't be you. As they move through the environment, they're searching, opening, and downloading data in patterns that don't match yours.

Varonis monitors user and data activity to alert on any suspicious or abnormal behavior that occurs across your sanctioned cloud applications. Using proprietary threat models and policies, you will receive detailed alerts on suspicious activity detected in your environment that may be putting your organization at risk.

These alerts include activities such as:

- When a user accesses or downloads an abnormal amount of sensitive data
- When sensitive data is shared publicly
- If a user logs in from an unusual or blacklisted country.
- If MFA has been disabled
- Excessive password/MFA reset requests
- If a contractor or stale account becomes active after a long period of inactivity

These are just a few of our many alerts generated by our threat models which we are constantly (and automatically) updating and evolving based on research from Varonis Threat Labs.

Identify org-wide misconfigurations and protect admin accounts

While attackers are after your data, they are also looking to identify which accounts will give them the widest access to sensitive data and organization-wide misconfigurations or weak configurations that they can exploit.

Hackers will target your privileged and admin accounts as they not only have access to more data but also have the rights to change configurations within the cloud platform that will make it easier to steal sensitive data without being caught.

Ensuring that you configure admin accounts correctly and constantly monitor their activity is vital. Suppose you spot an admin performing suspicious actions, like changing SSO settings, removing the need for MFA, changing passwords, granting increased access to other accounts, or other risky privileged activity without the knowledge of others. In that case, that may be a sign of a threat.

It is also considered best practice to have your admins only use their privileged accounts to perform administrative task and use a different unprivileged users for daily actions such as accessing their files. This will help reduce the severity of an attack in a case where an admin account is breached.

Cross-cloud monitoring

Lateral movement has evolved in the cloud to include hopping from one cloud service to the next to maximize the impact of attacks. Threat actors often use credentials found in one cloud application to gain access to another—as seen with LAPSUS$—so it is critical to monitor all your cloud data stores and track how your users move across them so you can spot this type of lateral movement.

Takeaways

LAPSUS$ has shown us that it's never been easier for novice threat actors to do significant damage in a short period of time. As cybercrime becomes more lucrative, technical talent will continue to be drawn into the dark side and insiders will be tempted to sell their access. For defenders, it's absolutely critical to evaluate your cloud visibility and behavior-based detections—two things that have proven to be necessary to detect and prevent LAPSUS$-style intrusions and data exfiltration.

If you'd like to evaluate your cloud security posture and identify where you're at risk to threats in the cloud, Varonis offers engineer-led risk assessments free of charge. Each assessment comes with a free trial of our software and complimentary incident response services.

splunk>

Splunk's Top 5 SIEM Trends to Watch in 2022

Security incident and event management (SIEM) technology has been around for years, with the core capabilities of the platform dating back to over a decade ago. Since then, SIEM solutions have evolved from a log management tool into an information platform, with demands from the enterprise driving much of the SIEM market. Just in the last few years, the SIEM market grew from $2 billion to a staggering $4.1 billion. Research from leading market analysts also found that the cost of data breaches is likely to exceed $5 trillion by 2024. That's almost double the amount reported in 2019, which totaled a cool $3 trillion. But thanks to the newer capabilities of SIEM software, organizations can mitigate this type of risk, and stop most (if not all) threats before any serious damage is done. The Gartner Magic Quadrant for Security Information and Event Management highlights these trends, as vendors continue to innovate and iterate on their SIEM software.

With so many exciting features on the horizon, here are Splunk's five SIEM trends to watch in 2022:

1. Cloud and app security will continue to be a top priority. 2. There will be a greater focus on risk-based alerts. 3. Threat intelligence and in-product security content are now critical. 4. Automation increases efficiency, productivity and response. 5. Insider threats will be easier to identify and respond to.

1. Cloud and app security will continue to be a top priority

With cloud adoption on the rise — largely due to COVID-19 and mass migrations to a remote workforce — a modern security solution has become critical to companies both big and small. Businesses have started to transition to the cloud at an incredible rate, and as more and more organizations turn to cloud infrastructures, the demand to upgrade and implement a cloud strategy becomes even more pressing. The technical complexities of migration are only one of the challenges an organization will face on their journey to cloud nativity. As teams sprint ahead with digital initiatives, they'll overlook general security requirements in an effort to beat the competition and accommodate shifting priorities. This ultimately leads to an increase in risk — especially if the organization is not up-to-date on network controls, access management systems or cloud configuration options. Coupled with an expanding attack surface and lack of visibility, a breach is just about imminent. Which is exactly why a robust SIEM solution should have out-of-the-box (OOTB) cloud security monitoring content — making it easier to detect and respond to threats across hybrid, cloud and multicloud environments. This could also include sophisticated detection rules for cloud attacks, and a vast cloud attack range to continuously test and improve cloud detections. In the age of remote work, a SIEM solution needs to be able to capture and analyze all cloud and endpoint data — regardless of volume, variety and

velocity. Traditional monitoring is no longer enough; security teams need to analyze and ingest data from a wide range of sources, across all types of environments in order to detect the where and why of security events.

2. There will be a greater focus on risk-based alerts

Alert fatigue continues to plague unwitting analysts on a daily basis. Alerts based on broadly defined detections can lead to a high volume of false positives and a lot of extra noise within a security operations center (SOC), quickly overwhelming and overburdening anyone on the front lines. Unsurprisingly, SIEMs need to get better at the effective detection and response to targeted attacks and breaches. Risk-based alerting (RBA) specifically — a newer methodology for identifying threats — attributes risk to users and entities, triggering an alert once certain behavioral and risk thresholds are exceeded. Security teams can then reduce the volume of alerts — while increasing true positives — surfacing sophisticated attacks that traditional searches often miss. This type of behavior profiling, threat intelligence and analytics in a SIEM can exponentially improve detection success by freeing up time and resources to hone in on complex, high-fidelity threats. Analysts can also attribute risk to various entities against their chosen industry-standard cybersecurity framework, like MITRE ATT&CK, the NIST framework and more.

3. Threat intelligence and in-product security content are now critical

Maintaining and evolving a security program's rules isn't easy. With so many disparate sources — as well as a wide array of data structures and formats to sift through — leveraging the necessary intelligence can be tedious and time consuming, especially when security teams have little-to-no bandwidth for creating the detections and playbooks needed. But nowadays, a modern SIEM solution can integrate threat intelligence (i.e., curated in-product security research around existing and emerging threats) into every stage of the incident response flow, as well as across an ecosystem of teams, tools, peers and partners. The guidance provided helps users preempt attacks and create complex pipelines without ever having to write or maintain scripts in the backend. Finally, thanks to the rapidly growing intelligence marketplace — which features all types of open, commercial and community intelligence sources — SIEM solutions are better able to incorporate the latest technical guidance and contextual awareness (like who's behind the attack and what their techniques are) that analysts can use step-by-step for investigating and responding to an alert.

splunk>

Splunk's Top 5 SIEM Trends to Watch in 2022

4. Automation increases efficiency, productivity and response

Some security tasks are just too big and too tedious for teams to process manually. Not to mention, the security skills shortage makes it difficult to find (let alone hire) talent in proportion to an organization's workload. Unsurprisingly, analysts often experience burn out while more pressing threats go unnoticed. In order to maximize productivity, efficiency and speed — and to not risk anyone's sanity — the only way forward is automation. Enter security operations, automation and response (SOAR). Now, most SIEM solutions are expected to integrate SOAR to eliminate analyst grunt work and resolve security incidents in record time, cutting their response from minutes (or hours) to mere seconds. A SOAR tool does this by weaving together intelligence from multiple tools, enriching alert data and surfacing it into a single interface. By automating the process of data collection, the analyst can see valuable details related to the alert as soon as it surfaces. Bottom line? Orchestration and automation helps security teams investigate and respond to security alerts much, much faster, and also enriches the data they collect through compiling intel from various sources into one place. By orchestrating decisions and actions to quickly investigate, triage and respond to a high volume of alerts, security teams can swiftly determine the risk level and respond accordingly.

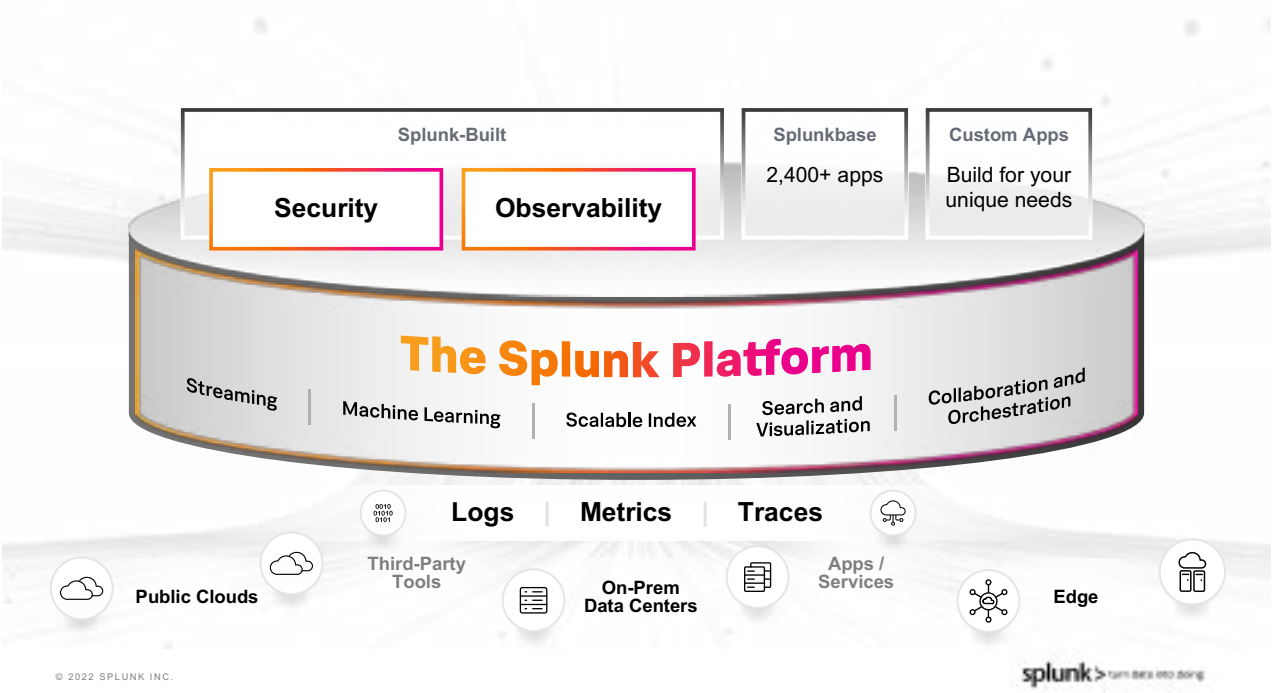
5. Insider threats will be easier to identify and respond to

Because insider threats are the hardest to catch — and potentially the most damaging — user and entity behavior analytics (UEBA) have long been a vital tool for detecting suspicious patterns that may indicate credential theft, fraud and other malicious activity. In essence, UEBA identifies and follows the behaviors of threat actors as they traverse enterprise environments, running data through a series of algorithms to detect actions that deviate from user norms. Historically, UEBA was adopted as part of a phased approach; organizations would start with a core SIEM, then eventually expand to UEBA and/or SOAR (and beyond). But now, UEBA is considered a key capability by Gartner, and should be working in concert — and ideally, as seamlessly as possible — with a SIEM solution to provide insights into behavioral patterns within the network.

By combining the power of both technologies within one platform, organizations reap the benefits of threat detection techniques that examine both human and machine behavior. Having UEBA as part of your SIEM means you can better recognize behavioral anomalies, as well as have additional context around known and unknown threats. This can save analysts' time and increase your team's efficiency by eliminating false positives and only surfacing high-fidelity threats that can't typically be detected through rules-driven correlation.

splunk>

Splunk is the data platform leader for security and observability. Our extensible data platform powers enterprise observability, unified security and limitless custom applications. Splunk helps tens of thousands of organizations turn data into doing so they can unlock innovation, enhance security and drive resilience.



Discover cyber exposures that lead to successful ransomware attacks and prevent them in advance, with the XM Cyber Attack Path Management

Ransomware groups are looking for ways to reach your critical assets, to increase their chances of getting a higher ransom payout. For the same reason, they have begun employing the double extortion technique, where before encrypting your data, they exfiltrate it and then threaten to leak it online. Searching for routes to reach your critical assets, attackers are lying low, propagating the network as a result of misconfigurations, unpatched vulnerabilities and mismanaged credentials.

Existing security controls are often siloed and provide fragmented visibility of your critical assets and the attacker's journey. Attackers take time to explore your cyber exposures but knowing which exposures put your critical assets at risk above others is challenging. Knowing what to fix first and which junctions in your network can be more damaging than others as many attack paths traverse through these is key to sabotaging any attack. Focusing on the attacker's path results in better resilience as well as better ROI from your existing security tools.

Get the attackers' perspective of your environment

The XM Cyber Attack Path Management Platform runs continuous and safe ransomware attack modeling, enabling you to see your environment through the eyes of the attackers and to gain complete visibility of the actual attack surface. By assuming breach, the platform highlights the cyber exposures that enable attackers to stealthily move within your network, on their path to take control of your critical assets, and to exfiltrate and encrypt data.

Early visibility of all possible ransomware attack paths and cyber exposures in your network will help you prioritize and focus resources on fixing the security issues that have the biggest impact on the success or failure of a ransomware attack.

- Illuminate and disrupt ransomware attack paths, in the cloud or on premises
- Close the gaps ransomware groups can use to compromise your network
- Continuously monitor and know what to fix first to prevent attacks
- Efficiently reduce the risk and impact of ransomware attacks

Highlight choke points

The key devices and entities that many attack paths traverse through and facilitate access to your critical assets and data.

XM Cyber

Ensure safe, fast and cost-effective remediation

XM Cyber Attack Path Management solution automatically generates an actionable remediation plan that prioritizes the required actions for cost-effective, safe and speedy disruption of current and future ransomware threats. Follow the step-by-step guidance to ensure optimized use of resources for fixing exposures, as well as continuous enhancement of your security resilience and improved operation of your existing security tools. It could be as simple as removing a user from the directory. Follow the step-by-step remediation plan to harden your environment and improve your security posture.

The XM Cyber Attack Path Management Platform proactively makes it harder for ransomware and malicious groups to access, exfiltrate and encrypt your data, by greatly reducing the attack surface, disrupting attacks in the making and enhancing your resilience.

Want to learn more?

Contact us by emailing **christine@xmcyber.com**

mimecast®

Relentless protection starts here.

Stop cyber threats before they affect your business.

Bringing Vulnerability Management to the next level

A single cloud-based app for a true risk-based vulnerability management program

qualys.com/**VMDR**

Qualys.

VECTRA®

Know Your Enemies – (Network) Behavior Gives Away the Attacker. Every Time.

Teppo Halonen

As the new reality of the continual dangers of cyberwar gradually sets in, organizations globally are working to harden their defenses. Most cyber-attacks are blocked by preventative safeguards. Highly motivated attackers, however, tend to find ways to get through those defenses.

Nation-state actors (APTs) sometimes use their access to novel vulnerability exploits (zero-days). They have vast resources at their disposal and can perform social engineering or can even physically gain access to their targets. Organized cybercriminal groups, on the other hand, may try to leverage insiders in their target organizations to mount their attacks.

Regardless of the threat actor – the attackers' behavior is similar

When an attacker has succeeded in gaining a foothold in the target environment, it is critical to detect them before they can compromise the entire system in a breach. Every attack starts with an initial compromise, by which time the attacker has likely achieved the following goals:

1. Gotten the ability to "live off the land" in one or more devices or services within the environment
2. Gained access to valid credentials
3. Evaded defensive measures such as identity management, firewalls, IDS, antivirus software, and even EDR solutions
4. Started to proceed toward their ultimate objectives by executing their "Cyber Kill Chain"

Depending on the target organization and the attacker in question, the end-game may be:

- Sabotage in some form
- Espionage, encrypting and/or exfiltrating data
- Stealing resources or committing fraud

VECTRA®

Know Your Enemies – (Network) Behavior Gives Away the Attacker. Every Time.

Teppo Halonen

Before the attacker can reach this end-game, however, they invariably – regardless of their goals – take the following actions toward the objective:

- Ensure resistance in the environment
- Secure a remote connection (C2) to the environment
- Perform reconnaissance
- Escalate access privileges
- Progress laterally toward the targeted high-value assets/data

The attackers obviously attempt to do all of the above while evading defenses and detection. But such actions along the kill chain create activities across the network – whether a physical, cloud, or virtual network.

AI has proven to detect malicious activities at scale and in real time

While the attacker's activities are hard to detect and distinguish from regular and safe activity, artificial intelligence (AI) has proven to be a good tool for doing this – at scale and in real time. Vectra AI does this by watching the network for patterns of attacker's behaviors – based on individual steps as well as the overall progression of the attack. Unlike other cyber-defense solutions, Vectra can spotlight attackers by detecting what they are doing across networks and systems – not just by detecting tools, signatures, IOCs, or anomalies but their concrete behavior.

Vectra does this across the on-prem networks and cloud (IaaS, SaaS, and PaaS), leveraging purpose-built, patented machine learning and AI – covering 97% of the MITRE ATT@CK network-based techniques.

Find out more: **www.vectra.ai**

Demystifying XDR: How Curated Detections Filter Out the Noise

Jesse Mack

Extended detection and response (XDR) is, by nature, a forward-looking technology. By adding automation to human insight, XDR rethinks and redefines the work that has been traditionally ascribed to security information and event management (SIEM) and other well-defined, widely used tools within security teams. For now, XDR can work alongside SIEM — but eventually, it may replace SIEM, once some of XDR's still-nascent use cases are fully realized.

But what about the pain points that security operations center (SOC) analysts already know so well and feel so acutely? How can XDR help alleviate those headaches right now and make analysts' lives easier today?

Fighting false positives with XDR

One of the major pain points that Sam Adams, Rapid7's VP for Detection and Response, brought to light in his recent conversation with Forrester Analyst Allie Mellen, is one that any SOC analyst is sure to know all too well: false positives. Not only does this create noise in the system, Sam pointed out, but it also generates unnecessary work and other downstream effects from the effort needed to untangle the web of confusion. To add to the frustration, you might have missed real alerts and precious opportunities to fight legitimate threats while you were spending time, energy, and money chasing down a false positive.

If, as Sam insisted, every alert is a burden, the burdens your team is bearing better be the ones that matter.

Allie offered a potential model for efficiency in the face of a noisy system: managed detection and response (MDR) providers.

"MDR providers are one of these groups that I get a lot of inspiration from when thinking about what an internal SOC should look like," she said. While an in-house SOC might not lose money to the same extent an MDR vendor would when chasing down a false positive, they would certainly lose time — a precious resource among often-understaffed and thinly stretched security teams.

Got intel?

One of the things that MDR providers do well is threat intelligence — without the right intel feed, they'd be inundated with far too much noise. Sam noted that XDR and SIEM vendors like Rapid7 realize this, too — that's why we acquired IntSights to deepen the threat intel capabilities of our security platform.

Demystifying XDR: How Curated Detections Filter Out the Noise

Jesse Mack

For Allie, the key is to operationalize threat intelligence to ensure it's relevant to your unique detection and response needs.

"It is definitely not a good idea to just hook up a threat intel feed and hope for the best," she said. The key is to keep up with the changing threat landscape and to stay ahead of bad actors rather than playing catch-up.

With XDR, curation is the cure

Of course, staying on top of shifting threat dynamics takes time — and it's not as if analysts don't already have enough on their plate. This is where XDR comes in. By bringing in a wide range of sources of telemetry, it helps SOC analysts bring together the many balls they're juggling today so they can accomplish their tasks as effectively as possible.

Allie noted that curated detections have emerged as a key feature in XDR. If you can create detections that are as targeted as possible, this lowers the likelihood of false positives and reduces the amount of time security teams have to spend getting to the bottom of alerts that don't turn out to be meaningful. Sam pointed out that one of the key ways to achieve this goal is to build detections that focus not on static indicators but on specific behaviors, which are less likely to change dramatically over time.

"Every piece of ransomware is going to try to delete the shadow copy on Windows," he said, "so it doesn't matter what the latest version of ransomware is out there – if it's going to do these three things, we're going to see it every time."

Focusing on the patterns that matter in threats helps keep noise low and efficiency high. By putting targeted detections in security analysts' hands, XDR can alleviate some of their stresses of false positives today and pave the way for the SOC to get even more honed-in in the future.

Find out more: **www.rapid7.com**

8 Reasons Why EDR is Not Enough

February 8, 2022 | Karen Crowley

Endpoint Detection and Response (EDR) tools have risen in popularity based on the belief they can stop and remediate most of the cybersecurity threats organizations face daily. But mounting evidence is painting a very different picture of EDR's efficacy and protection abilities. During the same period EDR has become a mainstay of modern security postures, attacks have skyrocketed in frequency, severity, and success.

The threat landscape is getting demonstrably more hazardous. Between 2019 and 2020 we saw an 800% increase in ransomware attacks and Ponemon Research has indicated that 80% of successful breaches come from previously unknown malware and zero-day attacks. The tools that many organizations are using are not providing adequate protection from increasingly sophisticated attacks.

And if EDR tools alone were the answer to preventing ransomware and zero-day threats we would see attacks trending downward. Instead, despite billions in spending, we're seeing them consistently rise.

Read the eBook: **8 Reasons Why EDR is not Enough** to learn why EDR tools are not the answer to defending against advanced attacks.

1. "Assume Breach" mentality is flawed
2. EDR is a reactive approach
3. EDR is not winning against ransomware
4. EDRs produce high false positives
5. ML weaknesses lower EDR's efficacy – and can be exploited
6. EDR is only as good as its visibility across every endpoint
7. EDR blocks post-execution, it doesn't prevent pre-execution
8. XDR only makes EDR less effective

Re-thinking Cyber Defense

EDR is based on an "assume breach" mentality – the long-held conventional thinking that no cyber defense can truly prevent cyber criminals from entering an environment. Detection and Response solutions like, EDR, MDR, NDR and XDR all have one thing in common – they are all based on post-execution remediation. By its very name, EDR is only relevant once the attack has taken place. And this ultimately means that the attackers are inside your network and you can't be sure you stopped the full context of the attack.

8 Reasons Why EDR is Not Enough

February 8, 2022 | Karen Crowley

Post-execution is too late to prevent a breach and remediation is costly and time consuming – a point driven home by recent research testing the efficacy of 11 of the best-known EDR tools highlighting their inherent shortcomings. The growing sophistication of modern threats and the high number of successful breaches has proven that EDR is not enough to stop today's increasingly advanced threats.

It's time to redefine what threat prevention truly is and explore new technology based on deep learning that has made malware detection, classification, and prevention possible.

Stop Responding. Start Preventing.

Security teams recognize that their security capabilities are not protecting them from today's most advanced threats and are actively investing in greater protection. Gartner forecasts that global security and risk management spending would exceed $150 billion in 2021. It likely surpassed that.

A prevention-first approach to stopping threats will complement or replace existing EDR solutions to mitigate risk. Preventing malware pre-execution and lowering false positives will improve operations, lower costs, and stop known, unknown, and zero-day threats, including ransomware, before they get the chance to infect your environment.

Download our latest eBook, 8 Reasons Why EDR is Not Enough, to understand why fresh thinking around EDR tools is overdue. And why deep learning-based cybersecurity holds the promise of true prevention, stopping >99% of threats and significantly lowering false positive alerts to <0.1%.

Find out more: **www.deepinstinct.com**

3 reasons to transform your security with XDR

Trellix

Imagine if your business could consolidate security tools into a holistic ecosystem that's always learning and adapting to keep you safe.

With extended detection and response (XDR), you can. It empowers you to identify and address incidents, simplify complex security products, and build a reliable security infrastructure.

Here are three reasons organizations adopt XDR:

1. Strengthen detection, response, and protection

As threat actors and attacks continue to evolve, risk management is becoming increasingly complex. Your organization must be able to detect and respond to threats in real time, powered by the right tools and insights.

20.9 hours

The average time to respond to a global incident is **20.9 hours**[1]

31%

Cyberattacks increased **31% from 2020 to 2021**[2]

2. Improve productivity

The security operations center (SOC) often has limited staff but an overwhelming number of security tools to manage. This hurts productivity and speed when you need it most—to stay ahead of growing threats.

70%

By 2025, **70%** of organizations will consolidate the number of vendors securing the life cycle of cloud-native applications to a maximum of three vendors[3]

3/4

By 2025, three-quarters of large organizations will be actively pursuing a vendor consolidation strategy, up from approximately one-quarter today[4]

3. Lower total cost of ownership

Organizations want to increase security operations efficiency. But buying best-of-breed products and building custom solutions is costly, and they may not be resilient enough for the future security landscape.

70%

70% of organizations have invested or plan to invest in XDR[5]

50%

By 2027, **50%** of midmarket security buyers will leverage extended detection and (XDR) to drive consolidation of workspace security technologies, such as endpoint, cloud, and identity[6]

Ready to breathe new life into your business with XDR?

Visit trellix.com to get started today. Or talk to one of our XDR experts to learn how Trellix can help grow your business.

1. Voice of SecOps, Deep Instinct, 2021
2. State of Cybersecurity Resilience 2021 , Accenture, 2021
3. Predicts 2022: Consolidated Security Platforms Are the Future, Gartner Research, 2021
4. Security Vendor Consolidation Trends—Should You Pursue a Consolidation Strategy? Gartner Research, 2020
5. ESG Research Highlights: Impact of XDR in the Modern SOC, Mandiant
6. Predicts 2022: Consolidated Security Platforms Are the Future, Gartner Research, 2021

Trellix

How Trellix is rewriting the security story

Trellix is at the forefront of the XDR revolution—pioneering a brand-new way to bring detection, response, and remediation together in a single living security solution. Our innovative XDR ecosystem:

- Empowers you to instantly analyze data and predict and prevent attacks with a solution that's always learning and adapting
- Enables you to create open partnerships and native connections to automate security policy orchestration
- Supports you with embedded tools and expert insights to reduce complexities and increase efficiencies

Experience a new, unified approach to XDR

Trellix XDR seamlessly integrates with our broad portfolio of endpoint, email, network, cloud, and other security products. It also easily connects with third-party security apps. This connectivity equips your business with intelligent threat sensing, analytics, and automated response. With a more unified experience, you have the power to:

Detect advanced attacks across all vectors:
Trellix XDR enables you to detect security incidents with confidence. Surface insights from multi- vector telemetry across multiple assets, throughout your organization, and apply that information to thwart attacks at scale.

Move from attack detection to threat prevention:
Trellix XDR blocks inbound email, network, and endpoint attacks. With a smart, adaptive ecosystem, you can predict and prevent emerging threats, identify root causes, and respond in real time.

Embed next- generation security into your operations:
Trellix XDR provides guided investigation workflows. By putting increased intelligence at the heart of your operations, you gain the ability to automate processes and prioritize your most critical security concerns.

Breathe new life into your business with Trellix

To forge ahead in the future, you need to protect your present. That means making sure your teams can be proactive, not just reactive. That your business is free to seize opportunities. That you finally have the upper hand over threats.

Trellix XDR combines innovative technology with the power of human expertise to:

- Create a more resilient digital world by rapidly adapting to the constantly changing global threat landscape
- Turn today's threats into tomorrow's advantages by correlating disparate events from multiple tools into actionable insights
- Embark on a brighter business future by reducing organizational risk through automated threat detection and response

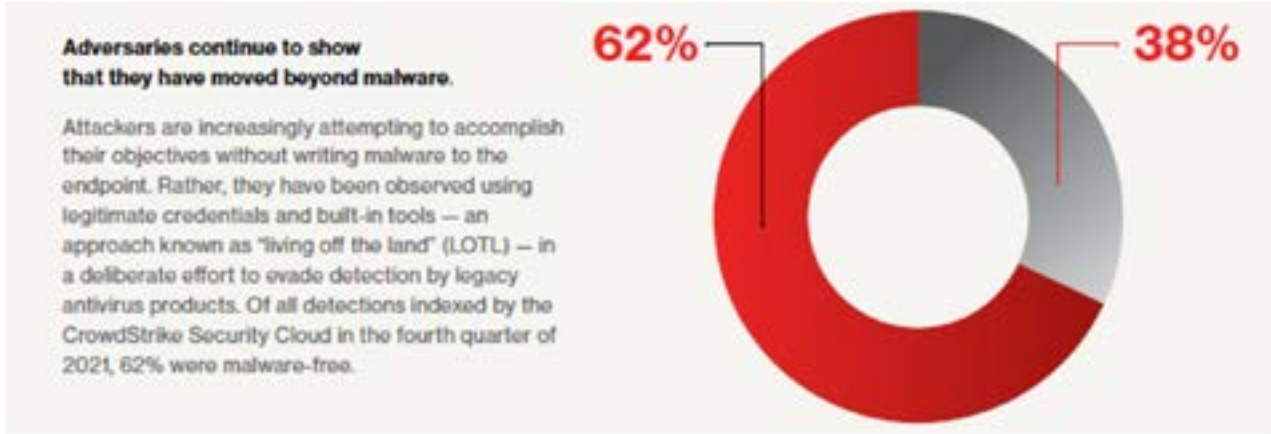
Ready to breathe new life into your business with XDR? Visit trellix.com to get started today. Or talk to one of our XDR experts to learn how Trellix can help grow your business.

Contact: Pat O'Leary | pat.oleary@trellix.com |+353 877 446 966

CROWDSTRIKE

Your Current Endpoint Security May Be Leaving You with Blind Spots

Threat actors are continuously honing their skills to find new ways to penetrate networks, disrupt business-critical systems and steal confidential data. In the early days of the internet, adversaries used file-based malware to carry out attacks, and it was relatively easy to stop them with signature-based defenses. Modern threat actors have a much wider variety of tactics, techniques and procedures (TTPs) at their disposal. CrowdStrike's 2022 Global Threat Report reveals **62% of attacks involve non-malware, hands-on-keyboard activity that will easily evade most legacy solutions, which are simply blind to this type of malicious activity.**

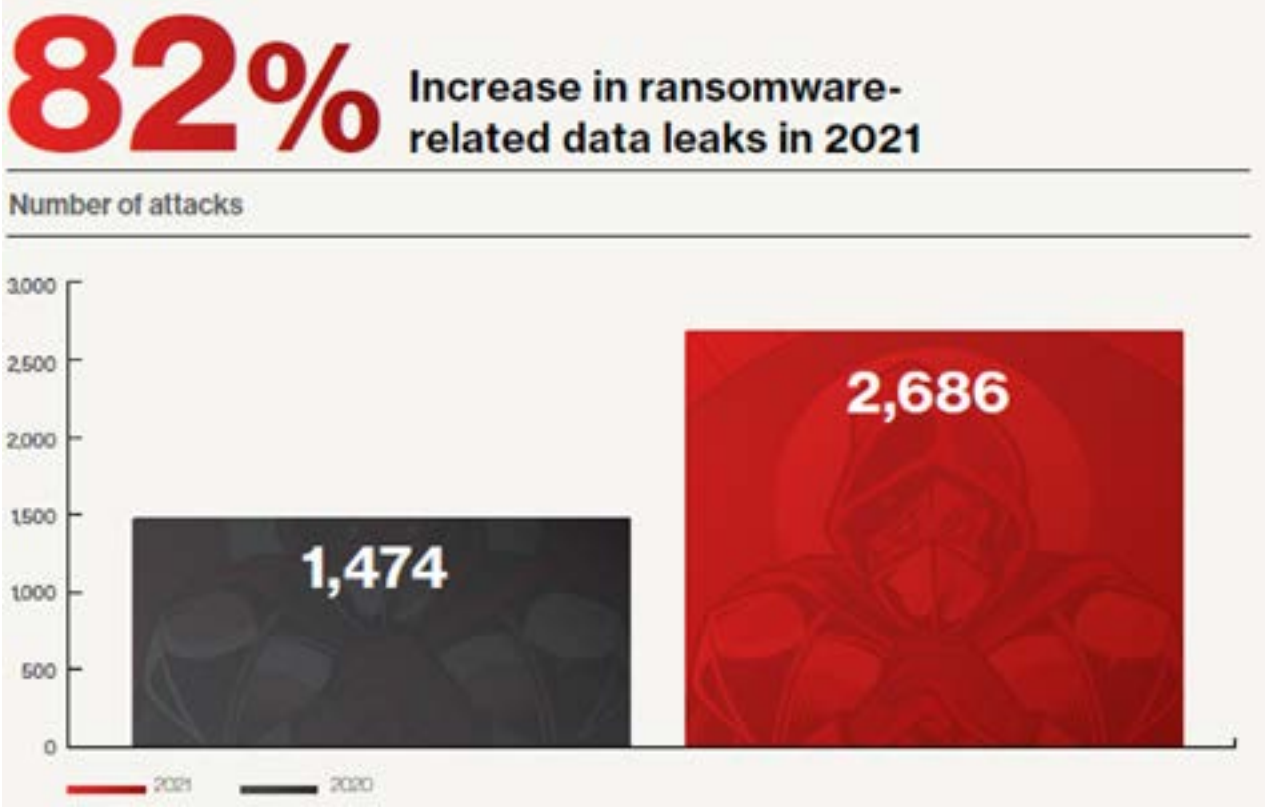


CROWDSTRIKE

Your Current Endpoint Security May Be Leaving You with Blind Spots

Today's savvy threat actors exploit endpoint vulnerabilities and use stolen credentials and fileless malware to penetrate systems and move laterally across a network to wreak havoc. Once they breach a network, sophisticated attackers can fly under the radar for weeks or longer, living off the land to actively plan and execute their moves. The incredibly sophisticated SUNBURST attack, for example, went undetected for nine months, impacting over 18,000 organizations across the globe.

Advanced threats like ransomware can paralyze your business and tarnish your company's reputation. The evolution of ransomware also reflects how adversaries are adapting their techniques and shifting their objectives. Many cybercriminals, no longer content to simply hold your data for ransom, now use ransomware to harvest data and reap additional awards. In fact, according to the CrowdStrike 2022 Global Threat Report, ransomware-related data leaks increased 82% in 2021.



CROWDSTRIKE

Your Current Endpoint Security May Be Leaving You with Blind Spots

Are You Still Fighting Yesterday's Battles?

Legacy endpoint security products like antivirus solutions were developed years ago to protect traditional IT environments and block rudimentary file-based malware. Antivirus solutions offer limited protection in the cloud era and no real visibility or protection against sophisticated threats that don't use malware. They are fraught with limitations, including:

- **Protection gaps.** Traditional antivirus clients rely on a central server deployed in a corporate data center to stay current with the latest threats. Today's cloud-first workers are often disconnected from the corporate network for extended periods and are unable to communicate with the server, which weakens protection and opens the door for threat actors.
- **Software lags and lapses.** Conventional antivirus clients are notoriously difficult to update. It can take weeks to roll out a routine software upgrade across the entire business. In the meantime, the organization may be exposed.
- **Performance and support barriers.** Traditional "thick" antivirus clients consume CPU, RAM and disk resources. They can degrade endpoint performance, impair user experience and burden the help desk with support issues.
- **Blind spots.** Conventional antivirus solutions are designed to protect individual endpoints against file-based malware. They don't gather or analyze security data holistically across endpoints to identify or block actions symptomatic of a modern attack like credential theft and lateral movement.

Learn more about what legacy endpoint security really costs.

Eliminate Blind Spots with CrowdStrike Falcon

CrowdStrike's cloud-native endpoint security solution is built from the ground up to eliminate blind spots and protect against today's sophisticated attacks. CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes and technologies that drive modern enterprise. Purpose-built in the cloud with a single lightweight-agent architecture, CrowdStrike's endpoint security provides unmatched scalability, superior protection and performance, reduced complexity and immediate time-to-value.

Powered by the CrowdStrike Security Cloud and world-class artificial intelligence (AI), the CrowdStrike Falcon® platform leverages real-time indicators of attack (IOAs), threat intelligence and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation across every customer endpoint in real time.

CROWDSTRIKE

Your Current Endpoint Security May Be Leaving You with Blind Spots

Designed for the digital era, CrowdStrike Falcon is delivered as a 100% cloud-based service that requires no on-premises hardware or software. The Falcon platform enables Day One deployment and on-demand scalability, and provides a single cloud-based administrative console. Easy-to-use APIs provide interoperability with other security platforms and tools to simplify security operations.

Falcon's cloud-delivered, universal lightweight agent runs on a wide range of endpoints and operating systems including workstations, servers, virtual machines and desktops, containers, mobile devices and Internet of Things (IoT) endpoints. Ideal for today's cloud-centric businesses, the Falcon agent requires no corporate network or VPN connectivity, and supports physical devices like PCs and bare-metal servers as well as virtual endpoints running in private or public clouds.

Falcon can help you eliminate antivirus blind spots, strengthen your security posture and reduce risk.

Next Steps

Legacy endpoint security solutions are no match for today's savvy threat actors. It's time to say goodbye to your old antivirus software. Try CrowdStrike Falcon for free today. Want more information? Join our CrowdCast, Focus on 5: Critical Capabilities for Modern Endpoint Security, to see a firsthand demo of the Falcon platform.

WHY WORK WITH INTEGRITY360

Security should be First with any project involving IT. From moving to the cloud to deploying a database, you need the people, processes and platforms to support a secure and seamless transition.

Integrity360 specialists are experienced with a wide array of tools, frameworks and projects. With a variety of certifications and years of industry-specific experience to their name, they're able to tackle any problem or challenge head on.

Contact an Integrity360 advisor today to learn more about our services.

HEAD OFFICE
3rd Floor, Block D, The Concourse, Beacon Court,
Sandyford, Dublin 18, D18 P6N4 , Ireland
+353 1 293 4027

UK OFFICE
46 New Broad Street, London, EC2M 1JH
+44 203 397 3414

Horizon Trade Park, 4 Ring Way, London, N11 2NW
+44 208 372 1000

NEW YORK OFFICE
260 Madison Avenue, 8th Floor Manhattan, 10016, USA
+1 212 461 3286

Integrity360
your **security** in mind

Useful Resources

Scan the code below to get access to the Integrity360 Resource Library.

Services

Managed Security

24x7x365 cyber security expertise to help you identify, mitigate, and protect against current and future cyber threats, while empowering your business to remain flexible and scalable. All without the cost and complexity of having to provision and manage it in-house.

Cyber Risk & Assurance

Cyber Risk and Assurance can help you achieve a wide variety of results through a methodical approach that looks at the risks you face from every angle, including digital and physical.

Cyber Security Testing

Cyber security testing helps you identify critical vulnerabilities that are being actively used to launch cyber-attacks. By quickly resolving these vulnerabilities, you can shut down exploits that would otherwise lead to an entirely preventable security incident.

Technical Consulting

Our security experts can become an extension of your own team, fill your skills gaps and help you remain agile and adapt to changing business needs and threat landscapes.

Technology

We work closely with world-class vendors to help our clients identify, implement and operate the security platforms that can help your business fend off unique threats.

Notes

#SecurityFirst2022

Integrity360

your **security** in mind

WWW.INTEGRITY360.COM