SECURING FINANCIAL SERVICES VR

7th July 2021
Online

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Securing banking's rush to the Cloud

e-Crime & Cybersecurity Mid-Year Summit 2021

"Thanks, very enjoyable. Look forward to my invitation to the March event. Thanks to everyone making this possible in these difficult times. I actually spent the whole day on it!"
Director of Global Security, American Express

"It's been a wonderful experience to attend this virtual conference. Many thanks for organising the event."
Information Security Officer/ Data Protection Manager, Jein Solicitors

2020 sponsors included:

Strategic Sponsors

BeyondTrust
CROWDSTRIKE
DARKTRACE
Menlo Security
proofpoint
RANGEFORCE
SentinelOne

Education Seminar Sponsors

bitglass
Centrify ZERO TRUST PRIVILEGE
corelight
Google Cloud
INTSIGHTS Defend Forward
KENNA Security
MORPHISEC Moving Target Defense
netwrix
okta
Recorded Future
Synack
TERRANOVA SECURITY
yubico

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

With banking fully online, security teams must provide unshakeable resiliency frameworks in the face of ever active threats.

The list of global banking institutions that are embracing public or hybrid cloud is increasing. This trend follows a period of fumbling reticence on the part of financial institutions to fully digitise. But this trepidation may be understandable: cloud security is a whole new territory for CISOs in the financial services. Security teams, the business and regulators need to tread carefully in order to make sure that banking in the cloud is secure.

Pressure has been added by FinTech upstarts who have challenged traditional banking frameworks. So too has the past 16 months of rapid digitisation. During the same period, numerous global financial institutions have successfully been attacked – ransomware waits in the wings for those hitherto considered too big to fail.

The stakes have never been higher for security teams in finance. Cloud migration is a necessity; attackers launch barrages on the banks; resiliency must be designed: are CISOs up to the task?

Join us for the second edition of the Securing Financial Services Summit to find answers to these pressing issues. In these regrettably now-precedented unprecedented times, it is more important than ever to share insights, resources and standards best practice. At the event expect to hear from the leading voices in cybersecurity from across the financial services in the UK and beyond. Please utilise our chat function and networking sessions and if you have any questions do not hesitate to get in touch with a member of the AKJ team.

Will Kaye | Editor

@eCrime_Congress **#ecrimecongress**

7th July 2021

Online

SECURING FINANCIAL SERVICES VR

Editor:
Will Kaye
e: will.kaye@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
t: +44 (0)7950 270 051
e: will.kaye@akjassociates.com

SECURING FINANCIAL SERVICES VR

In financial services, corporate execs and VIPs need added cyber protections

As security teams continue to struggle with data breaches, how can they thwart attempts to attack these important organisational leaders?

Like all security teams, those within the financial services space work around the clock to defend their organisations against cybercrime. Indeed, they have plenty to worry about at the organisational level. However, financial services security teams have an added concern: In the past few years, the exponential increase in and adaptation of attacks directly relating to corporate executives and other VIPs.

Cybercriminals target financial services executives and VIPs because they harbour sensitive information and have access to high-value assets. Cybercriminals also know that they can be impersonated to extract information from employees or customers.

Protecting executives' credentials, personally identifiable information (PII), assets, and data is an imperative component of any effective cybersecurity strategy. But as security teams continue to struggle with data breaches and weaponised leaked credentials, how can they thwart attempts to attack these important – and vulnerable – organisational leaders?

Understanding the types of threats to executives and VIPs

Hackers use numerous types of attacks when targeting corporate leaders, ranging from phishing schemes to malware drops designed to gain network access and beyond. The following are some of the most common attacks against executives and VIPs:

- *Data breaches:* Whenever corporate credentials are exposed in data breaches, security teams face a serious problem. Hackers can perform credential stuffing with massive databases of credentials, using brute force to gain entry to private networks and systems. The issue becomes exponentially more damaging when credentials belonging to admins or company executives are included. As IntSights researchers found in September 2019, cybercriminals can auction off admin credentials to networks, portals, and other corporate systems for significant amounts of money because they offer attackers unfettered access – as well as the ability to infiltrate a system without being detected. Similarly, company executives typically have access to higher-priority and exponentially more sensitive data than other employees. If leaked, their credentials can be used to execute disruptive attacks across entire organisations.
- *Malware and ransomware:* When hackers infiltrate a corporate network using admin or other VIP credentials, they can install malicious applications to exploit vulnerable company computers, compromising the organisation's security. In many instances, hackers use malware to demand a ransom from hostage businesses. While larger enterprises likely have teams in place to deal with this kind of attack – or at the very least, can afford to pay the ransom – this kind of attack can be devastating if preventative protocols are not in place.
- *Phishing and spear phishing:* Phishing is one of the oldest and best-known methods hackers use to attack businesses, governments, and consumers alike. And yet, despite its prominence, people remain incredibly susceptible to it. Ever-evolving and increasingly sophisticated phishing campaigns create nearly identical corporate digital assets – fake web domains, spoofed emails, social media accounts, etc. – to dupe consumers and employees into providing sensitive information and unwittingly offering access to corporate networks. Attackers use spear phishing to target specific employees who have access to sensitive information and are often successful in fooling them.
- *'Whaling' or CEO fraud:* A lesser-known form of phishing is 'whaling', or targeting the biggest 'fish' in a given organisation – the CEO, another high-level executive, or a board member. Whaling campaigns are designed to closely impersonate the selected VIP's online persona – whether it be via email, social media, or other form of corporate communication – to trick employees into performing a specific action. Generally, this action is something that gives attackers access to sensitive data or a confidential internal corporate system, or, in some cases, the means to carry out financial fraud. Whaling is also a type of social engineering.

Cybercriminals target financial services executives and VIPs because they harbour sensitive information and have access to high-value assets.

IntSights reports

A crucial component of successful threat intelligence gathering is real-time monitoring. Threat hunters can't possibly be expected to have ongoing visibility into every forum or black market where cyber-attacks are brewing.

- *Social engineering:* In addition to phishing tactics like whaling, cybercriminals use impersonated social media accounts and fake duplicate websites to lure unsuspecting customers and employees. By creating virtually indistinguishable websites with domains that appear to be legitimate, attackers can often fool the most discerning users. The prevalence and open nature of social media have also left many susceptible to social engineering scams. Hackers can fake an executive's LinkedIn or Twitter account with relative ease – all they need is a headshot and the information from the executive's actual accounts. They can then use these fraudulent accounts to impersonate the executive and dupe followers into performing specific actions. In addition, cybercriminals often create accounts impersonating recruiters on LinkedIn that lure even phishing-savvy users into clicking malicious links or providing PII.

Identifying and validating legitimate threats

When hunting for intelligence specifically pertaining to corporate executives or VIPs, the sources that prove most useful could prove to be entirely different from those that are highly valuable for threats targeting the organisation in other ways.

A crucial component of successful threat intelligence gathering is real-time monitoring. Threat hunters can't possibly be expected to have ongoing visibility into every forum or black market where cyber-attacks are brewing. There is only so much security teams can do manually; automation is a must to identify relevant threats to an organisation's VIPs. An automated threat intelligence solution offers continuous monitoring, delivering needed visibility into the blind spots of human threat hunters.

But threat detection is just the first step. Security teams must also authenticate the validity and veracity of a threat to an executive or VIP. They must determine whether the intelligence gathered indicates an imminent threat or innocuous mention. Not all mentions of a VIP are malicious, but if a hacker indicates they have the CEO's login credentials for a sensitive corporate network, it's time to act swiftly.

Mitigating threats with external threat intelligence

Once a threat has been identified and validated, security teams must immediately move to mitigate it. Time is of the essence for VIP protection, and a cyber-attack may be even further along than it appears. If an executive is compromised, they can suffer extraordinary personal damages and potentially leave the organisation exposed to attack. As mentioned previously, VIP credentials can open incredible opportunities for high-level critical data requests, allowing unrestricted access to sensitive repositories of data.

Automated threat intelligence can identify and validate a threat at the source and provide the tools necessary to shut it down:

- *Real-time monitoring:* Automation can save countless headaches, and fraud protection is no exception. An automated threat intelligence solution can send security teams alerts for leaked credentials, spoofed domains and social media accounts, and stolen credit cards found across the clear, deep, and dark web. Bank account information and other PII is constantly sold on dark web black markets, and real-time monitoring gives security teams the ability to eliminate threats before they evolve.
- *Automated remediation:* Also mission critical is the ability to automatically remediate certain types of threat alerts depending on the source of discovery. This includes locking down leaked credentials, PII like social security numbers, or other sensitive documents found in dark web forums with the click of a button. Financial services organisations should seek out a platform with the capability to monitor individual people's assets, in addition to company and brand assets. □

This article includes excerpts from the IntSights white paper, 'Defending Corporate Executives and VIPs from Cyberattacks'.

okta

Smart money starts with smart identity

Discover Okta solutions for financial services

okta.com/uk/financial-services

Open Banking and PSD2

Where are we now with global adoption, COVID-19 and the digital transformation; and what to expect next.

Jacquelyn Painter reports

As the banking industry continues to evolve – based on a multitude of factors including technology changes, touchless and contactless payment options, digital payment and banking innovation and applications, data security, and more – financial institutions are trying to keep up. These factors are commonly due to the changing and updated regulatory requirements, as well as consumer-driven services that rapidly change and modernise the way individuals bank and access information. This is happening across the globe in nearly every country on every continent – in various forms of disruption and evolution of digital innovations.

A digital paradigm shift: Open Banking and PSD2

One of these digital transformations is Open Banking and PSD2. The UK and European Union (EU) are leading the way on this in terms of implementation; and others in Asia Pacific, such as Australia, are also seen as early adopters for Open Banking based on market demands. A digital paradigm shift seems to be happening and it appears that this will only continue to grow – expanding in Asia, Latin America, and other areas as regulations and willingness to share data expands.

What is PSD2 and Open Banking?

- *PSD2* (also known as the second payment service directive) is a European Union regulation that requires all European banks to expose their customer account data to allow third parties to manage their finances through open APIs (application programming interfaces). PSD2 gradually started taking effect in January of 2018, however because of the security measures outlined in the Regulatory Technical Standard (RTS), and an extended deadline within the EU to implement PSD2's Strong Customer Authentication (SCA), it took until December of 2020 to fully implement – making it still very new to the banking industry.
- *Open Banking* (for both the UK and Australia) requires financial institutions to provide third-party access to customer account data with secure and open APIs. It is essentially the modern practice of sharing financial information electronically, securely and only under conditions that the customers approve of. The UK's Open Banking initiative took effect on 13th January 2018, aligning with PSD2. Australia's Open Banking requirements (also known as the Consumer Data Right or CDR) saw all financial institutions comply by July 2020.

Open Banking is growing

Open Banking revolutionises consumer banking, redefining it as a customer-centric ecosystem of banks and third-party providers. This system is fed by secure APIs that share consumer data – with customer consent. Many countries are beginning to have a heightened awareness to Open Banking due to the benefits it provides, in addition to regions implementing various forms of unique types of Open Banking regulations, industries and countries continuing to implement best practices for customer-centric solutions, and more.

In addition, the US is seeing some momentum as numerous banks and financial institutions already do business in the EU and must comply with Open Banking, the Financial Data Exchange (FDX) is gaining momentum in aiming to standardise various digital and Open Banking practices, and many US financial institutions are already collaborating with FinTechs. In addition, more data privacy laws continue to be enacted making the foundational digital and security architecture more viable to withstand and launch Open Banking.

Overall, Open Banking has many benefits, including:

- *Consumers:* Have a clear and centralised view of finances in one place – helping them budget, find deals and shop for products and services. In addition, it can streamline payments from banking to other services
- *Banks:* Expand offerings by opening APIs and connect and partner, alliance partners, and other service providers and platforms to integrate services. In addition, they can analyse customer behaviour for more personalised and relevant services through digitisation of banking services
- *FinTechs:* Quickly launch products and services in agile environments to compete and gain market share, expand collaboration with banks to broad portfolio, and integrate other platforms for added security

Does Open Banking rise to the top of the priority list because of COVID?

Although Open Banking progress differs from region to region, digital transformations/disruptions are taking hold even more due to the global COVID-19 pandemic given that many industries and organisations have had to pivot to digital platforms and ecosystems that work within an organisational

The benefits of being able to tie accounts together and securely access financial information (including banking, mortgage, investments and more) in one place has gained consumer momentum through the pandemic.

architecture and business strategy. There is no doubt that the pandemic has expedited technology transformations and digitisation and will continue to accelerate the Open Banking conversation.

In fact, recent research suggests that there has been a steady increase in adoption for Open Banking since the start of the pandemic. A study done by Open Banking Implementation Entity (OBIE) and Ipsos MORI state that the UK's small business community is utilising more services offered by Opening Banking to help future-proof their business operations, improve resilience, and keep up with the evolving and accelerated digital transformation that consumers are expecting with less face-to-face interaction and more streamlined approach to accessing various applications in the digital world.

The benefits of being able to tie accounts together and securely access financial information (including banking, mortgage, investments and more) in one place has gained consumer momentum through the pandemic. The key, however, is consumer confidence and buy in.

What to expect next: Considerations for banks

The consumer-friendly changes proposed by Open Banking standards pose significant challenges – and opportunities – for banks. PSD2 and Open Banking will open up the market to new entrants to give consumers more flexibility and choice on how to manage and spend their money. It is evident that digitisation of services will be critical for banks – no matter what region they are based or operate in. Being able to educate consumers on the benefits of sharing data confidently, as well as the value of an enhanced consumer experience will be crucial for adoption.

Banks will need to strike a balance that includes:

- Enabling frictionless user experience that includes transparent, streamlined experience with a dashboard-level control over solutions and data preferences
- Providing stronger, more restrictive security that includes the ability to scale and grow in a way that allows banks to be in continuous regulatory compliance
- Adopting a technology strategy that modernises banking platforms through collaboration with third-party providers and FinTechs
- Investing in innovation that allows for banks to embrace end-to-end digital architecture.

The Okta solution

Okta helps banks confidently innovate the customer experience through strong identity and access management and offers a PSD2 and Open Banking solution that meets the needs of the bank, as well as enhances the customer experience.

Through a world-class identity and access management solution, Okta enables banks to bring customers and employees a frictionless single sign-on experience, while protecting sensitive data with strong, adaptive multi-factor authentication that automates appropriate access across each end user's lifecycle.

In addition, Okta has strategic technology partners that offer dynamic authorisation governance that extends identity protections to APIs. This provides continual, contextual authorisation at a transaction level and ensures that APIs – both internal and external – are continuously monitored, and access is assessed based on risk and threat intelligence.

Banks and financial service providers need new tools to safely enable customer-centric Open Banking solutions. Contact us today to learn more about how we can help you. □

Jacquelyn Painter is Senior Solutions Product Marketing Manager for Financial Services at Okta. She is responsible for leading the company's financial services solutions to customers, and drives the strategy and messaging across the organisation. Prior to joining Okta, she has led multiple product marketing roles in high-tech and cybersecurity over the past 10 years.

For more information, please visit **www.okta.com/uk/financial-services/**

Accelerate time to value with the right cloud security strategy

Those who act swiftly will seize the opportunity to create a competitive advantage.

The pace of change

For financial services organisations, the world has fundamentally changed. Digitalisation and innovation, increasing regulations, demographic shifts, a complex global economic environment, increasing cost pressures, and – most importantly – rising customer expectations, are all mounting pressure to compel transformation.

The ability to successfully transform via disruptive innovation, new business models, delivery of tailored services, and improved customer experiences will separate progressive financial champions and leaders from the fold. Those who act swiftly will seize the opportunity to create a competitive advantage – enhance brand loyalty, attract new customers, and guarantee success.

To thrive in the future financial marketplace, priorities should include simplifying legacy systems, breaking down siloed business units to unlock valuable data, updating information technology (IT) operating models, taking software-as-a-service (SaaS) credentials beyond the cloud, adopting robotics and artificial intelligence (AI), and preparing the architecture to connect to 'anything, anywhere'.

However, legacy systems and infrastructure have been unable to support and keep up with current technological trends. The old paradigm of applications in data centres, with users connected in doesn't work in a world of clouds and smartphones. Systems must be capable of supporting the latest digital products, services, and applications that customers demand. This means that by shifting towards such systems, financial institutions can optimise the user experience and operate more flexibly and dynamically.

As a result, financial services organisations and their IT teams are facing the ever-increasing challenge of meeting the demands of the business at pace whilst complying with legislative guidelines and adhering to commercial constraints. This requires a new security paradigm.

The ability to successfully transform via disruptive innovation, new business models, delivery of tailored services, and improved customer experiences will separate progressive financial champions and leaders from the fold.

Challenges to factor in

New disrupters

With Open Banking levelling the playing field, financial institutions must rethink their business models to reinvent themselves and compete in future markets driven by open practices and a sharing economy. New and agile digital-native entrants are winning the innovation race as they do not inherit the technical debt and legacy infrastructure that so many incumbents need to consider. As a result, they can bring services and products to market faster and offer premium and tailored customer experiences grabbing more market and wallet share from incumbents. By offering services based on smartphones or tablets and running efficiently in cloud-based environments, they can deliver instant results to the customer.

Regulation

Financial services organisations need to conduct business in a highly regulated market and with the opening up of financial services markets, governments have introduced legislation in an attempt to protect all stakeholders. Rules on all aspects of the operation have come into force to ensure that the customer and business are protected from criminal activities. Where is the data? This is what regulators are concerned about, and it's more important now than ever before with online and application-based banking.

Security complexity

As markets open and partnerships develop within and across the industry, threats to the business and consumer have grown in complexity and number. With so much of daily life facilitated by smart devices, both access to the system as well as the data that is resident within the business must be protected. As financial institutions move to more flexible cloud-based services and environments, the need for a pervasive approach to security is required, with the ability to show real-time compliance now a mandatory feature. This all adds cost and complexity to the business.

Financial services organisations are developing and deploying services and applications in multiple clouds to gain the flexibility and agility required to play in the

Fortinet reports

new marketplace and meet the demands of the business and its customers. But how safe is the cloud, in particular when multiple providers are involved? What are some of the challenges IT teams are encountering when working in hybrid and multi-cloud environments?

Putting multi-cloud to the test

Cloud providers go to great lengths to protect their infrastructure, but protection of the business data and applications hosted or deployed in the cloud is the responsibility of the financial institution.

While there are small differences in how the shared responsibility model is represented between different cloud providers, the biggest difference lies in how native cloud security capabilities are implemented and managed. Each cloud provider offers different security services using different tooling and approaches. In this context, each public and private cloud – as well as the on-premises data centre – becomes an independent silo in a fragmented network security infrastructure – not an ideal proposal.

When working across multiple clouds, the ability to standardise, manage and automate security is the challenge that IT teams in financial services organisations are seeking to overcome. The major issues facing them include:

- With each cloud hosting a new set of services and management tools, supporting them becomes complex and costly for the existing IT infrastructure and administration teams.
- The greater flexibility clouds provide to instantiate new cloud workloads can make it difficult for IT teams to have full visibility of all workloads, let alone manage and secure them.
- Most financial institutions have a hybrid environment, but all regulatory mandates and basic security tasks still broadly apply, no matter where the workloads are running.
- Important as it is to demonstrate compliance, in a hybrid environment it is inefficient to use different solutions to manage or secure workloads, and to integrate data across various environments.

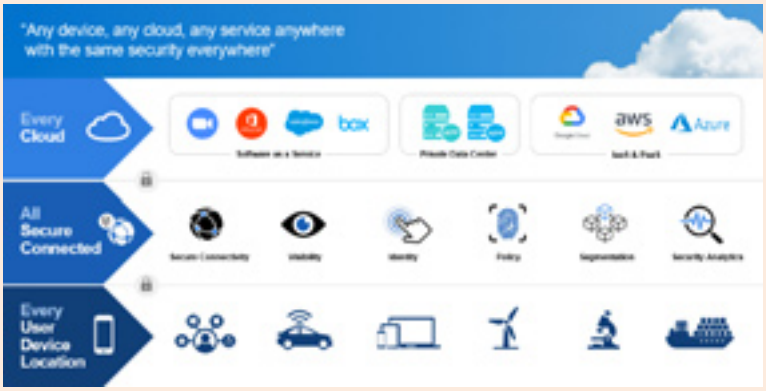
Key security elements for successful multi-cloud adoption

To leverage the advantages of cloud, financial services organisations must adopt a unified security architecture that runs across multiple cloud platforms and embodies the following key capabilities:

- Native integration with all major cloud providers
- A broad suite of security tools to cover the entire attack surface
- The ability to centrally manage the security infrastructure
- Automate security operations
- Visibility of the infrastructure, devices, and applications
- The ability to centrally control policy and for policies to be adaptive

To that end, a multi-cloud security approach that leverages the strengths of each cloud will become the new standard, ensuring every system runs optimally across a sprawling estate of service offerings. □

Fortinet's vision for a multi-cloud world you can trust



Fortinet's Adaptive Cloud Security extends a financial institution's security framework to all cloud services, thus providing the necessary visibility, policy enforcement, and automation across multiple clouds, and enabling secure applications and connectivity from an on-premise data centre and a distributed workforce to the cloud.

With our cloud security framework providing consistency, standardisation, and comprehensive protection, financial services organisations can benefit from the native security capabilities of each cloud while levelling up protection across the estate, improving risk posture and operational efficiency.

Fortinet's approach is to leverage cloud-native features with virtual solutions that deliver advanced security – such as next-generation firewalls, intrusion prevention systems (IPS), and end-to-end high-performance encryption and inspection. It means IT teams can protect cloud workloads, resources, applications, and data in the most dynamic cloud environments.

Also, we offer the largest ecosystem of partner integrations via APIs for broader visibility and a stronger end-to-end security solution.

With Fortinet security underpinning their cloud strategy, financial services organisations can innovate, accelerate time to value, and realise their future vision.

For more information, please visit
www.fortinet.com

FORTINET®

FORTINET®

Adaptive Cloud Security, everywhere you need it.

Protect the possibilities with Fortinet.

www.fortinet.com


Attackers start with people.
Your protection should, too.
Proofpoint protects your people, data and systems by stopping threats, training users and securing information everywhere it lives.
proofpoint/uk
proofpoint.
Protection starts with people.

Do you really know who is accessing your data?

How remote and hybrid working is changing the face of insider risks.

Rob Bolton reports

The COVID-19 pandemic posed an immediate challenge for cybersecurity teams globally. Within days, organisations were tasked with facilitating large-scale remote working, many for the first time. Staff suddenly took data and processes home that may never have been expected to operate outside of secure premises – and the cybersecurity team just had to 'make it work'.

This rush to maintain 'business as usual' during a pandemic came at a cost and, for many organisations, diluted their security controls, increasing their risk of a breach.

According to Proofpoint's recent Voice of the CISO Report, 59% of UK CISOs agree that remote working has made their organisation more vulnerable to targeted cyber-attacks, with 60% revealing they had seen an increase in targeted attacks in the last 12 months.

Cybersecurity teams, inhibited by pandemic-driven budgetary restrictions, did the best they could to control the risk, but many are playing catch-up in their attempts to protect a much-increased attack surface, and the changes in working environment have naturally led to changes in employee behaviour.

Many workforces globally are planning their return to office, whether it will be on a full-time basis, only part-time, or remaining fully remote post-pandemic. As a result, cybersecurity teams are faced with a new, complex challenge: how can they protect their organisation and employees in a hybrid working world? Forrester Research predicts that insider incidents will increase from 25% in 2020 to 33% in 2021, which suggests we are in the midst of a challenging time when it comes to insider threats.

So, how do these circumstances impact the cyber-vulnerability of your workforce? And how do these changes impact the potential risk of insider threats – those negligent, compromised, or malicious users within your business?

Whether or not it is deployed in a hurry, remote or hybrid working increases the risk of cyber-threats by placing a greater burden on your most vulnerable point of attack: your people.

Remote and hybrid working impact on negligent, compromise, and malicious insiders

Whether or not it is deployed in a hurry, remote or hybrid working increases the risk of cyber-threats by placing a greater burden on your most vulnerable point of attack: your people.

Against the backdrop of a global pandemic, this risk is elevated for several reasons. For one, in the rush to deploy cloud environments, there was little time to train users to operate in those new environments.

As a result, many are working remotely without the security awareness required to do so. Add to this the distractions of working from home, the decrease of regular communications that comes with working alone, and the malaise caused by an open-ended pandemic, and it's easy to see why the risk of a negligent insider threat has the potential to increase.

Users working alone, outside the professional confines of the office, are more prone to the type of errors seized upon by cybercriminals, however a negligent insider's actions can go beyond simply making an error.

May organisations are aware of the danger: 62% of UK CISOs still consider human error to be their organisation's biggest cyber-vulnerability.

However, this user 'negligence' is not the only insider threat exacerbated by remote working.

Collaborative remote working over the past year has forced organisations to open up systems to employees more than ever – ultimately giving them more access to critical data and information across multiple platforms than ever before. Organisations now need to establish how they can share information in a way that protects against data loss without compromising employees' ability to work efficiently and effectively in a hybrid manner.

Malicious insiders outside the usual confines of the office may find themselves presented with increased opportunity for malice, and they may also find it easier to extract data and cover their tracks.

Transparency and vigilance are key. It's vital that you know who has access to your data, and that you understand the context behind why and how they are accessing it.

Widening the scope of insider threats

With traditional network access patterns a thing of the past, the door has been opened to another nefarious insider – the external credential thief. Indeed, Verizon's 2021 DBIR showed that 61% of all breaches exploited credential data via brute force attacks, credential stuffing attacks, or credential data leaked and used later.

In this new, remote working environment, however, these external attackers have the opportunity to maximise their damage. Behaviour that may once have been flagged as suspicious may now go unnoticed, allowing anyone with credentials to penetrate your perimeter and masquerade as a legitimate user.

Once inside, the credential thief can harvest and leak data, disrupt systems, and plant malicious payloads. The longer they remain undetected, the more damage they can cause.

Suddenly, the insider threat is no longer just about insiders. Now it's about an organisation's ability to identify and differentiate between well-meaning employees, malicious employees, and malicious external actors all being active inside your network – where one is 'bending' a policy to meet an immediate customer requirement, and two are seeking to cause harm, by stealing data or planting ransomware.

Protecting from the inside-out and outside-in

Organisations must ensure the correct tools are in place to monitor and understand network activity and automatically flag suspicious and unusual behaviour, especially at this time of heightened access to data from multiple remote platforms.

Security teams must monitor users' network activity – flagging up repeat or unusual requests for system access to spot potential privilege misuse. Limit the printing and copying of sensitive data and only allow access to 'need-to-know' information with a legitimate reason. This will not only raise an alarm for improper employee use of data, but also potential external threats aiming to access your networks.

Organisations should implement and police policies regarding the use of email, acceptable use, external storage devices and the use of personal devices. These policies must be agreed to by anyone with access to your systems – employees, vendors, contractors and any other third party.

Transparency and vigilance are key. It's vital that you know who has access to your data, and that you understand the context behind why and how they are accessing it. The greater your understanding, the easier it is to spot irregularities or changes in behaviour – and the faster you can nullify potential insider threats, as well as those that are trying to siphon your data from the outside-in. □

Rob Bolton is Senior Director, Insider Threat Management, International at Proofpoint.

For more information, please visit **www.proofpoint.com/uk**

proofpoint.

The world has changed. Here's how to get the board to realise it

Requests to increase IT security budgets are often denied, and while many understand the need to move to the cloud, asking the board for additional budget to uproot the company's current IT infrastructure can prove difficult.

Jamie Moles reports

The rapid transition from on-premises to remote workforces in the wake of the Covid-19 crisis will be looked back upon as a world-historical event. For enterprise IT, it was an earthquake that fundamentally changed the landscape on which we stand.

When the pandemic hit, remote working was a trend that was already on the rise. However, even the most forward-thinking companies did not offer remote working for more than a generous handful of their employees. IT infrastructure was historically built for the castles and moats of yesteryear in which the large majority of those using the corporate network would physically be in the office. The future is hard to predict – but I think we can say with a high level of certainty – that the moat has dried up and most won't be going back to the castle.

Enterprise IT has changed dramatically in the last year, but that doesn't mean that the conversation has changed the boardroom. Requests to increase IT security budgets are often denied, and while many understand the need to move to the cloud, asking the board for additional budget to uproot the company's current IT infrastructure can prove difficult.

So how do we get to yes? First and foremost, let's admit that security practitioners and executives often see the world from two very different vantage points – it's difficult for many on the security side to translate their needs into a business outcome. To get the board on board – those points must converge.

Presenting the problems

You might think the mega breaches that regularly fill headlines are a useful reference point. However, using the widespread fear about breaches as a proof point is a blunt and inaccurate tool at best.

Security practitioners are better off focusing on how to convince executives of the objectives that are specific to their organisation, and concentrate the argument solidly around the concept of risk.

Dredging up fear and paranoia is not helpful, but constructive caution is. The board should understand the risk that exists and how it will impact the business. Examples such as new attack vectors or poor employee security practices have to be translated into how they directly affect the organisation. Speaking to the positive business effects from improved cybersecurity practices will win over talking technology.

The board won't expect you to fend off every single attack, but they should know that when the day does come – you'll lead with resilience. That doesn't always mean stopping the fires from ever starting, but that when the worst does happen, you are ready to slide down the pole and put the fire out before it causes severe damage.

Providing the solutions

The board's job is to think about the big picture, and oversee business objectives from the top down. From that lofty vantage point, it can often seem like security objectives are getting in the way of business agility. In order to get the board to understand your side you need to show them how security concerns and business objectives align, or better yet improve the bottom line.

Remote work is a perfect example of the relationship between security concerns and business objectives. In the past, remote work was marred by fears around productivity loss and weak controls over network access. Many of those fears have been alleviated over the steady acceleration of remote working throughout the world and businesses are starting to see remote working as a positive force. As such, many executives are now planning for a hybrid workforce.

The security concerns, although diminished, still remain. According to SANS Remote Workers Poll, 70.5% of remote workers access sensitive information from home. Without the correct solution

Security teams must learn how to consistently communicate with the board in the business language that they understand to change perception at the very highest level within your enterprise.

in place to ensure they can do so securely, employees will default to their own practices, devices, and preferred apps. This can create access headaches and a Shadow IT problem that can exacerbate security problems. With distributed networks and employees it becomes increasingly crucial to passively monitor your remote workforce and employ machine learning to automatically understand when behaviours are deviating from normal.

If the board's business objective is to maintain and ensure a productive hybrid remote workforce moving forward, then security personnel must be ready to help them understand the potential threats to the organisation, as well as employee productivity, and outline a plan that translates technology investments into business language.

When succeeding, security practitioners may be invisible to the business, but be very noticeable when they're not. Frequently seen as an obstacle to growth they need to be seen as a partner to the business. Security teams must learn how to consistently communicate with the board in the business language that they understand to change perception at the very highest level within your enterprise. □

Jamie Moles is Senior Security Engineer at ExtraHop.

For more information, please visit **www.extrahop.com**

Crypto-mining malware: Uncovering a cryptocurrency farm in a warehouse

Opportunistic individuals are using covert methods to hijack corporate infrastructure with crypto-mining malware.

Justin Fier reports

Cryptocurrencies are hitting the headlines every week and quickly becoming accepted as a mainstream investment and method of payment. Across the world, cybercriminals are leveraging data centres called crypto-mining 'farms' to profit from this trend, from China to Iceland, Iran, and even a cardboard box in an empty warehouse.

How does cryptocurrency mining work?

Cryptocurrencies are decentralised digital currencies. Unlike traditional currencies, which can be issued at any time by central banks, cryptocurrency is not controlled by any centralised authority. Instead, it relies on a blockchain, which functions as a digital ledger of transactions, organised and maintained by a peer-to-peer network.

Miners create and secure cryptocurrency by solving cryptographic algorithms. Rather than hammers and chisels, crypto-miners use specialised computers with GPUs or ASICs to validate transactions as quickly as possible, earning cryptocurrency in the process.

Crypto-mining farms in 2021: Reaping the early harvest

Crypto-mining takes up an enormous amount of energy. An analysis by the University of Cambridge estimates that generating Bitcoin consumes as much, if not more, energy than entire countries. For instance, Bitcoin uses approximately 137.9 terawatt hours per year, compared to Ukraine, which uses only 128.8 in the same period. Bitcoin is just one of many cryptocurrencies, alongside Monero and Dogecoin, so the total energy consumed by all cryptocurrencies is far higher.

Given that high-powered mining computers require so much processing power, crypto-mining is lucrative in countries with relatively cheap electricity. However, the energy needed can lead to serious consequences – even shutting down entire cities. In Iran, the outdated energy grid has struggled to provide for cryptocurrency farms, resulting in city-wide blackouts.

Crypto-mining malware has the ability to hamper and even crash an organisation's digital environment, if unstopped. Cyber-AI has discovered and thwarted hundreds of attacks where devices are infected with crypto-mining malware.

While some of these crypto-farms are legal, illegal crypto-miners are also straining Iran's energy supplies. Illegal crypto-mining is popular in Iran partly because Iranian currency is volatile and subject to inflation, whereas cryptocurrency is (for the moment) immune to both inflationary monetary policy and US sanctions. When used for illegal purposes, cryptocurrency farming can lead to network outages and serious financial harm.

Crypto-mining malware in corporate networks

Crypto-mining malware has the ability to hamper and even crash an organisation's digital environment, if unstopped. Cyber-AI has discovered and thwarted hundreds of attacks where devices are infected with crypto-mining malware, including:

- a server in charge of opening and closing a biometric door;
- a spectrometer, a medical IoT device which uses wavelengths of light to analyse materials;
- 12 servers hidden under the floorboards of an Italian bank.

In one instance last year, Darktrace detected anomalous crypto-mining activity on a corporate system. Upon investigation, the organisation in question traced the anomalous activity to one of their warehouses, where they found what appeared to be unassuming cardboard boxes sitting on a shelf. Opening these boxes revealed a cryptocurrency farm in disguise, running off the company's network power.

Had it remained undiscovered, the crypto-mining farm would have led to financial losses for the client and disruption to business workings. Mining rigs also generate a lot of heat and could have easily caused a fire in the warehouse.

This case demonstrates the covert methods opportunistic individuals may take to hijack corporate infrastructure with crypto-mining malware, as well as the need for a security tool that covers the entire digital estate and detects any new or unusual events. Darktrace's machine learning flagged the connections being made from the warehouse boxes as highly anomalous, leading to this unexpected discovery.

As bad actors continue to proliferate and hackers devise new ways to deploy crypto-mining malware, Darktrace's full visibility and Autonomous Response in every part of the digital environment is more important than ever.

In organisations with Antigena active, any anomalous crypto-mining devices would be blocked from communicating with the relevant external endpoints, effectively inhibiting mining activity. Antigena can also respond by enforcing the 'pattern of life' across the digital environment, preventing malicious behaviour while allowing normal business activities to continue. As bad actors continue to proliferate and hackers devise new ways to deploy crypto-mining malware, Darktrace's full visibility and Autonomous Response in every part of the digital environment is more important than ever. □

Justin Fier is Director of Cyber Intelligence & Analytics at Darktrace.

For more information, please visit **www.darktrace.com**

Cyber range and simulation-based training use case coverage

How a new generation of e-learning and simulation technologies is changing the way CISOs operationalise cybersecurity.

Next generation training to improve cyber-defence

Everyone is familiar with the three legs of cybersecurity: people, process, and technology. However, most investments of time and money go to just one area – technology. A growing investment in technology should not be a surprise when vendors continue to push technology-only solutions. At the same time, security training focuses mostly on end-users and social-engineering/phishing awareness. On a related note, there has been no easy, unified way to measure cybersecurity process or operational effectiveness. As a result, cyber-incidents continue to grow in number and magnitude.

RangeForce offers the industry's only integrated cybersecurity simulation platform that is focused on improving the skills of each security team member and how they work together. Critical new cybersecurity skills can now be learned in hours, rather than weeks, by team members at any time and anywhere. But the real value of simulation-based cybersecurity training does not stop there – it offers additional value to the cybersecurity organisation across seven important use cases, including visibility, hiring, onboarding, skills-building, and more.

Understanding and reporting cybersecurity effectiveness

Your board wants to know, your CEO wants to know, your compliance team wants to know, and you want to know – Can the security team handle a real cyber-attack that can steal from and even shut down my business? The answer to this question typically comes in the days and weeks following an attack. In its worst outcome, revenue and customers are lost, fines are levied, and careers ended. By focusing on continuous training, assessments, and simulation exercises and by capturing all of these activities in unified reporting, CISOs and security managers can build on strengths and remediate weaknesses. CISOs can then report an accurate assessment of a team's skills and a path to improvement to executives, and compliance teams to achieve confidence across an organisation.

Dealing with staffing shortages

Hiring experienced cybersecurity professionals is difficult and, for many, not an option. A robust approach to countering staffing and skills shortages is to build a flexible team through role-based cross-training. Following a military developed model where each member of a team is trained on multiple positions, CISOs can use RangeForce assessments and learning paths to identify their most proficient cyber-pros and cross-train them into other security areas. Cross-training decisions can be based on skills gaps, processes models, role timing, and technology employed. The goal is to optimise the roles covered by each team member at each stage in the detection and response process, so no one is 'sitting on their hands' at any time during an incident.

> "Due to our company location, we do not have a lot of local security talent to choose from. Utilising RangeForce for cross-training, especially our best IT folks, has allowed us to meet our security team resource requirements."

Improving hiring processes through assessment

When a company is looking to bring on new security talent, **RangeForce can improve the hiring process.** With the existing skills shortage, candidates are likely to be fresh out of school or through a cyber-training certificate programme. The candidates may not have the operational skills needed to effectively fill the role or the aptitude to be trained in the role. For this reason, security managers can no longer rely on a candidate's resume, training certificates, or professional references for qualification. What is needed is a way to assess a candidate's cyber-defence skills across a variety of attack vectors and security tools – RangeForce assesses cyber-defence skills across a variety of attack vectors and security tools.

Getting new hires up to speed quickly

When new cybersecurity team hires come on board, it often takes many months to train them into the role. Often, they are sent to vendor and third-party training, followed by months of on the job training, while shadowing a more senior member of the team already in the role. A recent Ponemon Institute survey[1] found that the time to hire and train one analyst is almost one year.

RangeForce reports

RANGEFORCE

RangeForce has developed a series of Cybersecurity Learning Paths that cover both introductory and advanced role-based skills development.

Starting with Security Operations Analyst (Level 1), a new hire completes approximately 30 hours of training customised to match the needs and tools of the role. The Learning Paths include simulation-based assessments so security managers can watch the learner's progress and assure required skills are being developed. Within weeks, the new hire can operate independently in their role, saving significant time and cost for the security team.

Career path development and improved retention

Cybersecurity leaders can improve the retention of valuable staff by building career paths that include increasing responsibility, training, and certificates. **RangeForce delivers learning paths that can be combined to create career paths for security staff.** Because these learning paths can be configured to the roles and tools of any cybersecurity team, they give team leaders a tool to build the career of a young analyst over multiple years and into new roles that the analyst is interested in obtaining.

Optimising security tool investments

RangeForce integrates leading security tools in both its hands-on training module coverage and in its Battle Fortress Cyber Range so that security operators can utilise their security stack. They learn through a series of lessons delivered in RangeForce training modules that take them from introduction to advanced usage. Then they move to the Battle Fortress Cyber Range to test and practice their skills on the tool until they are honed to a razor's edge.

Conclusion

If one of the most significant challenges facing cybersecurity is the shortage of and investment in human capital, then an investment in RangeForce is a wise decision. Initial testing on the RangeForce platform allows CISOs to assess where their company's staff is genuinely prepared for a variety of different cyber-attacks and where improvement is needed. Once employees' skills are assessed, RangeForce provides a turnkey solution: centrally administered training tools help address problem areas using state-of-the-art tools and approaches. Testing without training doesn't offer today's CISO with current data. Testing, followed by training, followed by additional testing, provides CISOs with hard evidence of how they are improving their company's readiness for an eventual cyber-attack.

CISOs at these forward-thinking companies have shifted investment from technology to people and adopted a strategy to improve cyber-readiness focused on:

- Role-based advanced cyber-defence training
- On-demand, interactive, hands-on lessons
- Standards-based (NIST/MITRE/OWASP) learning modules
- Simulated attack scenario training
- Individual & team skills assessments and reporting

What's preventing you from making the same investment in your human capital? □

[1] The Economics of Security Operations Centers: What is the True Cost for Effective Results? Ponemon Institute.© Research Report Sponsored by Respond Software Independently conducted by Ponemon Institute LLC. Publication Date: January 2020.

About RangeForce

RangeForce creates accessible cybersecurity training experiences for you and your team. Powered by the industry's first integrated training platform and virtual cyber range, we help customers operationalise a SaaS-based cybersecurity training program in hours, saving up to 65% over traditional training and up to $1m annually on hosted cyber ranges. RangeForce is revolutionising cybersecurity training with its adaptive learning technology to better train and cross-train DevOps, IT, and security professionals. Train with us to build cyber-resilience, and follow us on LinkedIn and Twitter.

For more information, please visit **www.rangeforce.com**

RANGEFORCE

RANGEFORCE

Upskill in an On-Demand Cyber Range

Experience hands-on and interactive cybersecurity training for you and your team. Start your RangeForce journey today and prove your strength against the latest cyber attacks.

rangeforce.com

Sponsors and exhibitors

Darktrace | Strategic Sponsor

Darktrace is a leading autonomous cybersecurity AI company and the creator of Autonomous Response technology. Its self-learning AI is modelled on the human immune system and used by over 4,700 organisations to protect against threats to the cloud, email, SaaS, traditional networks, IoT devices, endpoints, and industrial systems.

The company has over 1,500 employees and is headquartered in Cambridge, UK. Every second, Darktrace AI fights back against a cyber-threat, before it can cause damage.

For more information, please visit www.darktrace.com

ExtraHop | Strategic Sponsor

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Our breakthrough approach analyses all network interactions and applies cloud-scale machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises including Home Depot, Credit Suisse, Caesars Entertainment, and Liberty Global to rise above the noise of alerts, organisational silos, and runaway technology. Whether you're investigating threats, ensuring the availability of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

Learn more at www.extrahop.com

Fortinet | Strategic Sponsor

Fortinet makes possible a digital world that we can always trust through its mission to protect people, devices, applications and data everywhere. This is why the world's largest enterprises, service providers, and government organisations 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 centre to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 510,000 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 programmes in the industry to make cyber-training and new career opportunities available to everyone.

Learn more at www.fortinet.com, the Fortinet Blog, or FortiGuard Labs

IntSights | Strategic Sponsor

IntSights is revolutionising cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralise cyber-attacks outside the wire. Our unique cyber-reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defence has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo.

For more information, please visit intsights.com

Proofpoint | Strategic Sponsor

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber-attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

More information is available at www.proofpoint.com

Okta | Strategic Sponsor

Okta is the leading independent provider of identity for the enterprise, and the Okta Identity Cloud enables organisations to both secure and manage their extended enterprise, and transform their customers' experiences.

With over 5,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely adopt the technologies they need to fulfill their missions. Over 5,600 organisations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to securely connect their people and technology.

For more information, please visit www.okta.com

Recorded Future | Strategic Sponsor

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organisations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organisations around the world.

Learn more at recordedfuture.com

BeyondTrust | Education Seminar Sponsor

BeyondTrust is the worldwide leader in privileged access management (PAM), empowering organisations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organisations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organisations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including more than 70% of the Fortune 500, and a global partner network.

Learn more at www.beyondtrust.com

Centrify | Education Seminar Sponsor

Centrify delivers modern privileged access management (PAM) solutions based on Zero Trust principles to enable digital transformation at scale. Centrify provides modern least privilege access for human and machine identities based on verifying who is requesting access, the context of the request, and the risk of the access environment. Centrify centralises and orchestrates fragmented identities, improves audit and compliance visibility, and reduces risk, complexity, and costs for the modern, hybrid enterprise. Over half of the Fortune 100 trust Centrify, including the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. human or machine, in the cloud or on-premises, privileged access is secure with Centrify.

For more information, please visit www.centrify.com

LogRhythm | Education Seminar Sponsor

LogRhythm's award-winning NextGen SIEM Platform makes the world safer by protecting organisations, employees, and customers from the latest cyber-threats. It does this by providing a comprehensive platform with the latest security functionality, including security analytics; network detection and response (NDR); user and entity behaviour analytics (UEBA); and security orchestration, automation, and response (SOAR).

Learn how LogRhythm empowers companies to be security first at logrhythm.com

Menlo Security | Education Seminar Sponsor

Menlo Security protects organisations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

For more information, please visit www.menlosecurity.com

OneTrust GRC | Education Seminar Sponsor

OneTrust GRC enables risk, compliance and audit professionals to identify, measure, and remediate risk across their business to comply with internal rules and external regulations. OneTrust GRC is a part of OneTrust, the #1 most widely used privacy, security, and governance platform trusted by more than 9,000 customers and powered by 150 awarded patents.

OneTrust GRC is powered by the OneTrust Athena™ AI and robotic automation engine, and integrates seamlessly with the full OneTrust platform, including OneTrust Privacy Management Software, OneTrust DataDiscovery™, OneTrust DataGovernance™, OneTrust Vendorpedia™, OneTrust Ethics, OneTrust PreferenceChoice™, OneTrust ESG, and OneTrust DataGuidance™.

To learn more, visit OneTrustGRC.com or connect on LinkedIn

RangeForce | Education Seminar Sponsor

RangeForce develops the world's most comprehensive cybersecurity training and cyber-skills assessment programme. RangeForce believes in the power of skilling up SOC and cybersecurity professionals through advanced cyber-defence training, combining this with the ability to accurately and quantitatively assess your team's genuine preparedness to combat real cyber-attacks. Every day, hackers invent new creative techniques, with regulators administering increasingly significant fines. Using our Battle Skills individual training platform in combination with the Battle Fortress team event cyber-range, we help companies mitigate their cybersecurity risk and boost the effectiveness and efficiency of their security operations. Our advanced threat training covers the very latest attack and defence techniques, all delivered through a browser and on real infrastructure. No prep, no set-up, no testing, no kit, no downtime, no hassle. All you have to do is log in, learn, assess and transform – for a fraction of the cost of traditional learning.

For more information, please visit www.rangeforce.com

Red Sift | Education Seminar Sponsor

Founded in 2015, Red Sift is a global company providing cybersecurity services to organisations such as Wise (previously Transferwise), Telefonica, Pipedrive, ITV and top global law firms.

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. Products on the Red Sift platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analysing the security of inbound communications for company-wide email threat intelligence.

Find out how Red Sift is delivering actionable cybersecurity insights to its global customers at www.redsift.com

Virtru | Education Seminar Sponsor

Virtru is a global leader in data privacy and protection. We help organisations to take control of their data – everywhere it's shared – through end-to-end encryption for Google, Microsoft, and enterprise apps such as Salesforce, SAP, and Zendesk. Our flexible, easy-to-use, and trusted encryption technologies provide access controls, self-hosted key management, DLP rules, and persistent audit to meet the strictest privacy, compliance and data sovereignty needs. Over 6,000 customers trust Virtru for data security and privacy protection.

For more information, visit virtru.com or follow us on Twitter at @virtruprivacy

Zivver | Education Seminar Sponsor

Zivver provides outbound email and file transfer security to help public and private sector organisations stay compliant and prevent data leaks (80% of which is caused by human error).

It is the only vendor in the market to offer a complete outbound email and file transfer security solution, tackling all three phases – before, during and after, a communication is sent. The service also conveniently integrates with leading email clients such as Outlook and Gmail, so it's easy-to-use.

Trusted by more than 4,000 organisations of all sizes to safeguard important data, the user-friendly platform helps to improve regulatory compliance as well as business performance.

With Zivver, many companies quickly see a positive business case. That's why 98% of customers renew their service agreements, and the average rating on Gartner Peer Reviews is 4.6 out of 5.

The company continues to expand their portfolio to meet the evolving needs of the moment while also developing secure communication tools for tomorrow.

For more information, please visit www.zivver.com

SECURING FINANCIAL SERVICES VR

AGENDA

08:00 Breakfast networking

08:55 Chairman's welcome

09:00 **Two cases for measuring cyber-risk appetite**

Simon Collins, Director, Head of Cybersecurity, Allianz Global Investors, and **Brian Cooke,** CISO, Permanent TSB

- Join this session to hear two alternative approaches to measuring cyber-risk appetite
- One approach will focus on the sophistication of the attackers, the other will be based on key risk indicators
- Both approaches will be explored, followed by a discussion of the strengths and challenges of each

09:20 **Navigating enterprise security in a post-compromise reality**

Jamie Moles, Senior Security Engineer, ExtraHop

- Every organisation gets compromised – it's how fast you detect and respond to an incident that counts
- This is especially important when you look at trends like the overnight move to remote work, the rise in encrypted traffic and acceleration of cloud adoption, as well as the proliferation of enterprise IoT that have expanded the attack surface and complicated the job of security professionals
- We'll explore those trends and the opportunity that lay ahead for security teams post-compromise to prevent an event that results in an outage or an incident from becoming a full-scale data breach

09:40 **Q1 2021 Top vulnerabilities landscape**

Jason Steer, Director of EMEA Presales, Recorded Future

- Why Q1 2021 had the highest high-risk vulnerabilities since our report began
- Why your supply chain is your achilles heel
- Why COVID continues to shape the vulnerability landscape

10:00 **To resiliency and beyond!**

Steve Brown, Director, Cybersecurity, Mastercard

- Increasingly complex networks of business relationships are exposing participants to systemic operation risk
- As a result, our national security, public safety and economic growth are being exposed to major disruption
- In this session, see how Mastercard is delivering trust through an approach that quantifies, automates and prioritises risk to build cyber-resilience and trust throughout the connected digital economy

10:20 **Education Seminars | Session 1** **See pages 30 to 32 for more details**

BeyondTrust	RangeForce	Red Sift
Solving the cloud identity challenge	**Revolutionising cybersecurity training for your enterprise defence teams**	**DORA: why future proofing email security is essential**
Karl Lankford, Director, Solutions Engineering, BeyondTrust	**Rupert Collier,** VP Sales – EMEA and APAC, RangeForce	**Dr. Rois Ni Thuama,** Head of Cyber Governance, Red Sift

10:50 Break and networking

11:20 **Delegates will be able to choose from the following topics:**

Slips, lapses and mistakes – what your security awareness programme can't fix

John Scott, Head of Security Awareness, Bank of England

- Everyone knows by now not to click a suspicious email or to open a dodgy looking attachment. So why does it keep happening?
- This session will draw on the fields of health and safety and behavioural psychology to understand why teaching people what to do doesn't always help, and what you can do to make your awareness programme more effective

Why maintaining an on-prem paradigm in the cloud will not work

Luke Hebbes, Head of Risk and Cybersecurity, HSBC

- Banks used to be about the safe storage of your money and valuables, with physical safes and cash. Now the vast majority of transactions are electronic and banks (and other FS companies) are primarily technology companies. This was a different approach and requires a different mindset
- The technology isn't the same and the models don't work: addressing the switch from on-prem to the cloud
- Rapid adoption of SaaS and cloud can cause issues with unstructured data. How do you provide data integrity and full lifecycle data management in the cloud and prove it to the regulators/auditors?
- What in your threat model that indicates managing your own keys for a SaaS system is significantly reducing your risk?
- Addressing issues that appear when moving from a quarterly release cycle to cloud technologies and agile development with multiple intra-day releases

11:40 **Identity focused security: Why start with identity when mitigating risks**

Matt Bailey, Platform Specialist, Okta

- Identity focused security and how identity is foundational to the financial services industry
- Why you should start with identity when mitigating security risks
- Key challenges we face today from remote working to the rise in bad actors

12:00 **Cyber-intelligence empowering IT security audit for financial systems**

Chris Strand, Chief Compliance Officer, IntSights

- What is Cyber Threat Intelligence (CTI) and why is it important to the financial services industry
- How to use CTI to prioritise financial system security gaps and enhance security posture
- How your business digital footprint can help predict targeted threat patterns
- Understand how to use CTI findings to accelerate risk assessment and data privacy adherence through real examples from the field

12:20 **Avoid playing whack-a-mole with your cloud security**

Joe Robertson, EMEA CISO, Fortinet

- Cybersecurity for financial institutions in the new normal must solve an equation with multiple variables, lots of unknowns, and adversaries that can pop up anywhere
- Users and customers can pop up anywhere too – in a branch, in an office, at home, on the go
- Ditto applications: they can move from the data centre to a cloud to another cloud, and a single query can bounce around like a pinball
- This session will cover what is needed for a flexible cybersecurity strategy and how an agile and consistent multi-cloud strategy can protect you today and tomorrow

12:40 **Education Seminars | Session 2** **See pages 30 to 32 for more details**

Centrify	LogRhythm	Zivver
Privileged access management challenges when moving to the cloud	**Detection and response strategies for cloud security incidents**	**How the financial services sector can benefit from secure digital communication**
Nick Colin, Regional Sales Director – EMEA, UK&I, Centrify	**Daniel Crossley,** Sales Engineering Manager, LogRhythm	**Rick Goud,** CIO, Zivver

13:10 Lunch and networking

14:00 **Cybersecurity isn't just doom and gloom**

Jerome Walter, CISO, Digital Venture, Standard Chartered Bank

- Over the last 10 years, the transformation brought about by Agile development, cloud technologies and DevOps has created a number of opportunities for security to rethink and implement new cyber-hygiene strategies without slowing down the enterprise
- See how the IDEAS architecture framework helps reconcile security and innovation
- Exploring key metrics that help drive better organisational outcomes
- How new practices are emerging to enable continuous verification and collective learnings

14:20 **Insider risk: A CISO imperative**

Rob Bolton, Sr Director Intl at Information Protection, Proofpoint

- Data doesn't lose itself. People's actions whether negligent, compromised, or malicious are #1 cause of data related breaches
- Legacy tools miss early signs of data and insider risks and can't provide granular user context yet cause alert fatigue – costing firms $11.45m annually
- Drawing insights from past breaches, we will explore effective pragmatic practices to mitigate exposure and insider risk across your organisation

14:40 **Banking on cyber-AI: Neutralising threats before cyber-attackers strike gold**

Mariana Pereira, Director of Email Security Products, Darktrace

- We discuss, how advanced cyber-defence technology protects the entire digital estate in high-risk environments
- Learn how cyber-AI thwarted a spoofed chase fraud alert aimed at gathering information for fraudulent transactions
- Discover how attackers are set to supercharge social engineering techniques with offensive AI

15:00 **Education Seminars | Session 3** **See pages 30 to 32 for more details**

Menlo Security	OneTrust GRC	Virtru
Why SASE is primed to secure the evolution of finserv	**5 steps to overcome data overload**	**Ensure true privacy in the cloud with data-centric protection**
Tom McVey, Solution Architect, Menlo Security	**Nick Pavlichek,** Product Manager, OneTrust	**Rob McDonald,** SVP of Platform, Virtru, and **Mark Williams,** Customer Success, EMEA, Virtru

15:30 Break and networking

16:00 **Customer digital identity in the financial services**

Martin Ingram, Product Owner, Identity and Access Management, NatWest Group

- What is a customer digital identity?
- What are the benefits for both customers and the business?
- How does customer digital identity change identity and access management in FS firms?

16:20 **Securing FinTech organisations**

The tendency for global banks to move their infrastructure to the cloud has much of its origin in the pressure exerted by the FinTech upstarts who have revolutionised the financial services across the past decade. Finance is changing, and at the forefront of this change are digital native, cloud-first, data driven organisations. How, then, is the FinTech vanguard protecting its crown jewels?

Philip Edwards, Director, Global Head of Security, Revolut
Tiago Rosado, Head of Cybersecurity, Curve

16:40 **Are you cyber-insurance friendly?**

Laure Zicry, Head of Cyber Insurance Western Europe, Willis Towers Watson

- State of the cyber-insurance market
- Trends in claims
- Be prepared for an underwriting meeting

17:00 Closing remarks

17:05 Break and networking

17:30 Conference close

Education seminars

Throughout the day a series of education seminars will take place as part of the main agenda. Delegates will be able to choose to attend any of the seminars, all of which will provide vendor-neutral, hands-on advice. Seminars within each session run concurrently.

Session 1: 10:20–10:50

BeyondTrust

SESSION 1
10:20–10:50

Solving the cloud identity challenge

Karl Lankford, Director, Solutions Engineering, BeyondTrust

Today, many financial services organisations rely on multiple cloud services with their end users regularly consuming dozens, or even hundreds, of different SaaS applications. This great cloud migration has successfully enabled the increase in remote working and is accelerating digital transformation initiatives. But, more clouds also means more challenges. In addition to the fundamental cloud security issues, there's the additional complexity and interoperability issues arising from siloed identity stores, native toolsets, and conflicting shared responsibility models between cloud providers, creating an expanded attack surface that organisations need to address.

The identity challenge is the most important security problem for organisations to solve and is best accomplished by standardising the management and security controls across the entire IT ecosystem.

Join this session to learn:

- The most pressing cloud security risks
- Where native toolsets leave gaps in security that you must address
- How to implement 7 cloud security best practices with privileged access management (PAM) to vastly decrease your likelihood and scope of a cloud-related breach

RangeForce

SESSION 1
10:20–10:50

Revolutionising cybersecurity training for your enterprise defence teams

Rupert Collier, VP Sales – EMEA and APAC, RangeForce

Continuous professional development is crucial to keeping technically focussed teams ahead of the game. CISOs, VPs and Team Leads must also be able to monitor and assess skill levels within those teams, in order to identify any possible coverage gaps that could represent a threat to the organisation. They also need to ensure incident response best practices remain fit for purpose and that everyone can execute their role in the event of an emergency.

In this seminar you will learn:

- How cyber-defenders can continue to acquire and hone their skills entirely through a browser but still in a hands-on fashion
- How they can learn essential real-world skills in real networks and real VMs. From security operations to forensics to secure DevOps, modules cover a breadth of mission-critical topics
- How users learn to defend against advanced attacks, quickly recognise and fix vulnerabilities and develop muscle memory in how best to react when it happens in the real world
- How actionable insights and metrics about performance and skill levels of team members can help identify the cybersecurity superstars, both already in your organisation and amongst those that may want to join
- How a combination of self-paced learning together with pressurised group exercises is the best way to prepare your teams for every eventuality – at a fraction of the cost of traditional learning

Red Sift

SESSION 1
10:20–10:50

DORA: Why future proofing email security is essential.

Dr. Rois Ni Thuama, Head of Cyber Governance, Red Sift

The EU has recently proposed the Digital Operational Resilience Act (DORA), aimed at improving security standards within the financial sector. Scheduled to become law as early as September 2021, it means that financial entities must 'address any reasonably identifiable circumstance in relation to the use of network and information systems'. But what does this mean in practice, and will these measures really help to protect firms?

In this session, Dr. Rois Ni Thuama makes the case that DORA is a force for good and will help businesses to make better decisions, faster.

Dr. Rois Ni Thuama will cover:

- Current cyber-threats within the financial industry
- Due diligence and its positive correlation with business efficiency
- Why DMARC is necessary for protecting business email

Session 2: 12:40–13:10

Centrify

SESSION 2
12:40–13:10

Privileged access management challenges when moving to the cloud

Nick Colin, Regional Sales Director – EMEA, UK&I, Centrify

Only a few years ago financial services were wedded to the perceived security and ownership of on premise infrastructure. Times have changed. Now many organisations are cloud first. However, much of the on premises infrastructure will remain for many years to come. Moreover, with multiple cloud providers often being the normal, this adds further complexity to the management and security of the entire estate.

To fully benefit from rapid technological transformation, it is imperative that enterprises embrace strategies for safeguarding their infrastructure and services both during and after cloud migration. In this session, we will discuss common challenges and the tools and strategies IT and security leaders are finding most effective for managing a secure transformation to the cloud.

- Managing security in a hybrid environment presents challenges that on premise vaults are not able to manage effectively
- Identity remains one of the few aspects that an organisation retains control over in the cloud
- Leveraging identity for effective privilege access management in the multi cloud hybrid world delivers the best blend of secure access methods

LogRhythm

SESSION 2
12:40–13:10

Detection and response strategies for cloud security incidents

Daniel Crossley, Sales Engineering Manager, LogRhythm

Join Daniel Crossley, LogRhythm, Sales Engineering Manager, UK, to discover common security incidents that happen in AWS environments and gain helpful tips for detecting and responding to them.

In this session you will learn:

- Common security incident types in AWS
- The various log types in AWS
- Helpful response strategies

Zivver

SESSION 2
12:40–13:10

How the financial services sector benefits from secure digital communication

Rick Goud, CIO, Zivver

Organisations of all sizes have been accelerating their digital communication efforts, especially since the onset of COVID-19 and the shift to remote working. A common misconception is that digital security is complex, intricate and will require many changes in the way people work. But organisations struggle to combine security with usability, and they need both to reap the benefits of digital communication in terms of efficiency, higher customer engagement and satisfaction.

- A sharing of experiences of how COVID-19 accelerated the need for digital communication, and the challenges that brings
- Examples of how the right secure digital communication tools can lower your costs, increase efficiency, and improve stakeholder satisfaction
- Gain insight and perspective into international financial services organisations who have successfully embraced digital communications and achieved better risk mitigation, cost control and adoption
- Key takeaways: Resources to better equip yourself, your team, as well as your citizens, residents and patients in how to reap the benefits of secure digital communication both now, and in the future

Session 3: 15:00–15:30

Menlo Security

SESSION 3
15:00–15:30

Why SASE is primed to secure the evolution of finserv

Tom McVey, Solution Architect, Menlo Security

Few industries have changed as dramatically as financial services (finserv) in the last decade. Banking and financial transactions were once an exclusively in-person process, but today the vast majority of customers conduct their financial affairs digitally. Additionally, finserv employees are highly dependent on websites and cloud or SaaS apps to perform their

jobs, putting increased pressure on the security and reliability of these systems. To address the challenges presented by both a distributed workforce and accelerated digital transformation initiatives, there's a movement spurring on the adoption of secure access service edge (SASE) architecture, which assures cloud security with any new deployments.

Join this session to understand more about why this forward-thinking framework is considered key to converging the network and security functions within finserv organisations today.

What you will learn:

- Key insights and considerations on protecting employee productivity, preventing attacks, and optimising security operations for a distributed workforce
- Why the fundamentals of SASE matter to the future of networking and security
- How modern cloud-first solutions are critical to delivering on the promise of SASE security

OneTrust

SESSION 3
15:00–15:30

5 steps to overcome data overload

Nick Pavlichek, Product Manager, OneTrust

Every organisation is working to reduce the delay between issuing a risk assessment, receiving a response, gaining risk insight, and making a risk-based decision. Risk insights quickly lose value as time elapses from the initial assessment request. Businesses should leverage the digital workstreams to collect information as updates occur using data discovery tools to find, document, and classify in real-time.

Exploring your data universe can be an overwhelming exercise, giving you more information than you know what to do within certain circumstances. Using careful data classification methods and flexible risk formulas, organisations can map information to harness real-time updates through a data discovery engine to fuel and standardise risk at scale with the latest information.

In this webinar, we'll review how you can quickly connect enterprise data through automated data discovery and translate the data into meaningful risk insights.

Attend to learn:

- Identify data across business applications for the latest risk insights
- Automatically categorise information to deliver meaningful insights across risk, compliance, and your executive teams
- Explore a new way to aggregate and standardise risk using real-time data points

Virtru

SESSION 3
15:00–15:30

Ensure true privacy in the cloud with data-centric protection

Rob McDonald, SVP of Platform, Virtru, and **Mark Williams,** Customer Success, EMEA, Virtru

There's no argument as to the benefits of the Cloud – ability to scale easily, improved productivity, heightened collaboration fuelling innovation, growth and seamless customer experience. But whatever stage of the Cloud journey you are on, one constant remains – how do you ensure that sensitive data that demands privacy – investor and banking PII, corporate IP – remains private and secure, and protected from unauthorised access (including your cloud provider) wherever it is shared and stored?

Join this session to understand how by adopting a data-centric security strategy, you can protect and control access to the data itself – everywhere it travels.

- Differences between traditional, perimeter-focused data security policies and data-centric protection
- How to implement a data-centric strategy that supports compliance and data sovereignty needs
- How to empower employees to collaborate in the cloud with seamless and secure sharing □

Speakers and panellists

Matt Bailey

Platform Specialist, Okta

Rob Bolton

Senior Director, Information Protection, Proofpoint

Rob leads Proofpoint Information Protection across the international markets. The frequency, cost, and complexity with security events that involve an insider is increasing each year. Rob and his teams are working with customers and partners alike to provide a level of visibility and control around the risks associated with data loss and insider threats; with a focus on helping companies protect against risky behaviour, protect their data and IP, and reducing the investigation cycles. For almost 23 years, Rob has been working alongside some of the most recognisable companies in the world, helping to solve some of the most critical security and technological issues. Originally from Washington, DC, now residing in London, Rob is a published author, international sales and operations leader.

Steven Brown

Director, Cybersecurity, Mastercard

Steve is Mastercard's lead for cybersecurity. He is responsible for the implementation and integration of Mastercard's Cybersecurity Framework including data breach detection and cyber-risk assessment technologies and capabilities across all related stakeholders including issuers, acquirers, merchants and governments. Steve also works to build and maintain strategic relationships with both internal, external, private and public sector parties, working with global teams to understand the needs of customers and technology required to deliver applicable solutions. Prior to joining Mastercard, Steve was an Officer of the UK's National Crime Agency for 17 years where, as Head of Cyber Threat Intelligence, he led the UK's strategic response to cybercrime with overall responsibility for the collection, management, analysis and assessment of intelligence on the cybercrime threat to the UK. Steve ensured a proactive response to prevent and mitigate harm to UK individuals and business through assessed threat and risk management, working across government and industry to determine and detail the national and international response to cybercrime. Steve also served as the UK's Cyber Attaché to the USA during 2016–2019, embedded with the FBI Cyber Division at National Cyber & Forensics Training Alliance (NCFTA). Steve was responsible for diplomatic and political relationships and negotiations relating to the investigation of cybercriminality affecting the UK and USA.

Nick Colin

Regional Sales Director – EMEA, UK&I, Centrify

Nick is a veteran in the PAM arena working in the field for over 10 years. He has worked with many of the world's top financial institutions to deliver best of breed identity led privilege access management solutions.

Rupert Collier

Director of Sales – EMEA and APAC , RangeForce

Rupert Collier is Sales Director, International at RangeForce, and, over the last 20 years, has worked in product management and commercial roles at many leading companies in the cybersecurity and wider technology industries. Bilingual in German and English, Rupert is responsible for RangeForce's business development activity outside of the United States and will give you insights on how simulation-based training is helping organisations elevate cyber-skills, fill staffing gaps, and cost-effectively improve their security team's ability to detect, contain, and remediate cyber-attacks. You will get to see the simulation platform in action and learn how it makes it easier to orchestrate and personalise training for larger teams with a diverse range of skill sets.

Simon Collins

Director, Head of Cybersecurity, Allianz Global Investors

Simon is Head of Cybersecurity at Allianz Global Investors. He has over 20 years' experience in IT,

the last 14 of which have been focused on cybersecurity. Simon was previously a Director in EY's EMEIA Cybersecurity practice based in Dublin, where he spent his early years as an ethical hacker and investigating cybercrime. His later years were spent helping organisations protect themselves from cyber-attackers and keep them out of trouble in the first place.

Brian Cooke

CISO,
Permanent TSB

Brian is the Chief Information Security Officer for Permanent TSB. He has over 20 years' experience in cybersecurity & technology risk within the financial services industry both in Ireland and internationally. Brian is a Director with the Institute of Banking and holds a master's degree in Information Security from Royal Holloway, University of London. He is also a Certified Information Systems Security Professional (CISSP) since 2003.

Daniel Crossley

Sales Engineering Manager,
LogRhythm

Philip Edwards

Director, Global Head of Security,
Revolut

After a background in solution, technology and then security architecture, Philip led Information Security at a FTSE50 organisation, before a period of cloud security and enterprise security architecture advisory consulting for global retail and defence businesses. Philip currently leads the Information Security function at the financial 'superapp' company Revolut as it advances its goal of putting people's whole financial life at their fingertips

Rick Goud

CIO,
Zivver

Before co-founding Zivver, Rick Goud spent six years as a Healthcare Consultant for Gupta Strategists. He had studied Medical Information Science at the UVA and Care Management at Erasmus University. Additionally, he holds a PhD in Medicine from the UVA on the development, implementation and evaluation of healthcare support systems. Throughout his studies, Rick worked as a programmer. The idea to launch his own company was conceived during Rick's career as a Strategy Consultant. As a health industry consultant, he noticed that a wide range of sensitive data was being frequently handled within organisations; this included patient information, company performance, and legal documents. Many of his clients had questions about data security and how data was being re-used etc. He realised that there was a strong need for a secure communication solution to safeguard and manage sensitive data, and shortly afterwards, Zivver was born.

Luke Hebbes

Head of Risk and Cybersecurity,
HSBC

Luke Hebbes is a passionate information security leader with 20 years of experience ranging from building high-performing teams to delivering cutting-edge research. He promotes innovative, risk-based solutions rather than the formulaic application of industry standards or vendor solutions. Luke believes that it is essential to view security from the perspective of business critical assets and to adopt a pragmatic approach, not letting technology drive the security requirements. Security is a supporting service to most businesses and, as such, should be a transparent enabler, used to protect the business and its assets, whilst aligning the risk posture with value generation – effective security can only be delivered with an understanding of the business context.

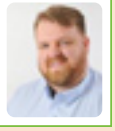
Martin Ingram

Product Owner, Identity and Access Management, NatWest Group

Martin Ingram is the Identity & Access Management Product Owner for NatWest Group, in charge of transforming identity & access management for RBS to support new customer and staff digital journeys. He has a particular interest in digital identity and how it will allow people to improve their digital lives while also managing the risks that organisations face. Prior to RBS, he has had a broad experience in security both from a vendor and a client organisation perspective having consulted or worked for organisations in Europe, America and Australia. As such, he has been involved in IAM, crypto systems, content security and malware amongst many other security domains. Martin has a background in engineering and has been on the board of several start-up technology companies.

Karl Lankford

Director, Solutions Engineering,
BeyondTrust



Karl Lankford is the Director, Solutions Engineering, for BeyondTrust, where he has worked for six years.

A highly capable security leader, Karl has acquired a wide range of security experience and knowledge over the last decade, working across multiple industries. Karl is a regular speaker at industry conferences, delivering disruptive technical and strategic thought-leadership insight to the international cybersecurity community.

Rob McDonald

SVP of Platform,
Virtru

Rob is the SVP of Platform and an advocate of safeguarding data across new applications and data-sharing workflows. Rob has also consulted with corporations to help them assess their current information security position and develop a plan to not only mitigate the discovered technical shortcomings but more critically to raise security awareness amongst their employees. Rob holds a bachelor of science degree in Computer Science from the University of Texas at Dallas and is a perpetual student of technology, information security, and privacy practices.

Tom McVey

Solutions Architect,
Menlo Security

Tom McVey is an EMEA Solutions Architect at Menlo Security, where he works to achieve his customer's technical requirements and architects web and email isolation deployments for organisations across many different industries. Coming from a background in UEBA & insider threat – he provides expert cybersecurity advice and strategic guidance to his clientele. Prior to Menlo, he always had a passion for cybersecurity and IT. In his spare time, Tom likes to play music and watch Formula 1 cars go around a track very quickly.

Jamie Moles

Senior Security Engineer,
ExtraHop

Jamie has worked in the computer industry for over 30 years, focused primarily on security and infrastructure technologies. In the early 1990s, Jamie was one of the UK's leading experts on computer viruses – authoring his own Virus Scanner for MSDOS before joining Symantec as Technical Support Lead for the new Peter Norton range of products, including the new Norton AntiVirus product. Nowadays, Jamie is helping customers understand and mitigate the risk contemporary threats pose to their business.

Rois Ni Thuama

Head of Cybersecurity Governance & Legal Partnerships, Red Sift

A doctor of law and an expert in the field of cyber-governance and risk mitigation, Rois is highly experienced in her role as Head of Cybersecurity Governance at Red Sift. She works with key clients across a wide range of industries including legal, finance, banking and oil & gas, and regularly writes and presents content focussed on significant cyber-threats, the latest trends and risk management.

Nick Pavlichek

Product Manager,
OneTrust GRC

Nick Pavlichek, GRCP, CIPP/E, CIPM serves as a GRC Product Manager for OneTrust GRC – a purpose-built software designed to operationalise integrated risk management. In his role, Pavlichek works to build the suite of GRC solutions that companies can implement and use throughout their risk management lifecycle. OneTrust GRC solutions support enterprise objectives, adopt industry best practices, and adhere to requirements relating to relevant standards, frameworks, and laws (e.g. ISO, NIST, SIG and more). Pavlichek works with clients to realise the extent of their risk exposure, helping clients to map their digital infrastructure, assess risks, combat threats, monitor ongoing performance, and document evidence throughout the risk lifecycle.

Mariana Pereira

Director of Email Security Products,
Darktrace

Mariana Pereira is the Director of Email Security Products at Darktrace, with a primary focus on the capabilities of AI cyber-defences against email-borne attacks. Mariana works closely with the development, analyst, and marketing teams to advise technical and non-technical audiences on how best to augment cyber-resilience within the email domain, and how to implement AI technology as a means of defence. She speaks regularly at international events, with a specialism in presenting on sophisticated, AI-powered email attacks. She holds an MBA from the University of Chicago, and speaks several languages including French, Italian and Portuguese.

Joe Robertson

EMEA CISO,
Fortinet

Joe Robertson represents Fortinet to the CISO

community, where he advises the executive committees of large enterprises and service providers as their digital transformation strategies require security-driven networks and holistic security approaches. In over four decades in the security and networking business, Joe has held technical, marketing, management, and executive roles at companies as diverse as Juniper Networks, Dimension Data, Bay Networks, IBM, and AT&T. He also founded and was on the board of directors of a network security startup.

Tiago Rosado

Head of Cybersecurity, Curve

Tiago is an acclaimed security professional with more than 22 years of information security experience across various sectors – banking, finance, FinTech, telcos, oil & gas, government, education, pharmaceutical, SaaS and ethical hacking. He is a seasoned strategic thinker and tactical implementer, skilled in developing strategies, goals, and methodologies for the cyber-defence programme in alignment with the industry best standards. Tiago has a vast record of success in building outstanding programmes with strong cultures that thrive on challenge, innovation, and opportunity in companies such as SensePost, giffgaff, Prosegur CyberSeguridad, Intralinks, VC Investments and Curve. He is a member of the CSFI – Cyberwarfare Division and a speaker at several conferences across Europe.

John Scott

Head of Security Education, Bank of England

John is a security educator with experience of running a team delivering face to face and online content to a diverse workforce, and is skilled in managing the move from awareness, to behaviour, to cultural change. He is an international public speaker on the subject of security culture. He has designed and delivered phishing and gamification campaigns. John is an IT Trainer with many years' experience in further and higher education, and in the public sector. He is skilled at course design and delivery.

Jason Steer

Director of EMEA Presales, Recorded Future

Jason Steer, Director of EMEA Presales at Recorded Future, has over 20 years of information security experience, having worked at a number of successful technology companies over the past 15 years, including IronPort, Veracode, and FireEye. Jason also has experience as a media expert with the BBC, CNN, and Al Jazeera, and has worked with both the EU and UK governments on cybersecurity strategy.

Chris Strand

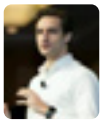
Chief Compliance Officer, IntSights

Christopher Strand is the Chief Compliance Officer at IntSights. As CCO, he is responsible for leading the global security risk and compliance business, helping companies bridge the gap between cybersecurity and regulatory cyber-compliance. Chris has more than 20 years of subject matter expertise in information technology and security audit assessment and he specialises in developing enterprise security platforms and markets within hyper-growth organisations.

Prior to joining IntSights, Chris launched and led the cyber-compliance business at Carbon Black (acquired by VMWare), and has held leadership and compliance specialist roles at other flagship security companies such as RSA, Trustwave, and Tripwire. His past experience has provided him with a unique insight in the areas of security assessment and audit, data security, forensics, threat intelligence and security solution implementation. Chris is trained as a Security Auditor, is a PCIP, and actively participates in the development of cyber-regulations globally. He is an active contributor and participant with ISACA, ISSA, ISC2, and the PCI SSC, frequently speaking on and publishing content advocating and informing the market on the evolution and alignment of their respective compliance frameworks. Chris graduated from the University of Guelph with a bachelor's degree in Environment Studies and completed advanced certificates in Computer Information Systems at Humber College Institute of Technology and Advanced Learning.

Jerome Walter

CISO, Digital Venture, Standard Chartered Bank



With more than 18 years of experience, Jerome is a forward looking and innovative security executive focused on leveraging best practices in IT and development to solve today's security and resilience challenges. Jerome recently joined Standard Chartered as the CISO for a digital venture. Prior to that, Jerome spent over two years accompanying the largest organisation's cloud-native transformation as Pivotal's Field CISO and VMware's Security Modernisation lead. Jerome also led security initiatives at Prudential Asia and Natixis in the Asia-Pacific region. He also held various positions as

Developer and Systems Engineer. Jerome holds a master of science in IT Engineering from EFREI, France, and an MBA in Finance from HKUST Business School.

Mark Williams

Customer Success Manager, EMEA, Virtru

Mark has over 10 years' experience helping enterprise organisations improve their security posture within the email security and data protection space. At Virtru, Mark leads the Customer Success team for EMEA and APAC, helping customers to optimise and innovate their approach to data protection. Mark holds a bachelor of science degree in Internet Computing from the University of Liverpool.

Laure Zicry

Head of Cyber Insurance, Western Europe, Willis Towers Watson

Laure is responsible for Cyber Insurance for Western Europe. She focuses on developing and delivering cyber-risk transfer solutions. Laure has extensive experience in cyber-risk management focusing mainly on related risk transfer solutions. Laure also has a background in financial lines insurance including directors and officers liability, professional indemnity and crime. Laure is a regular speaker at industry events, has been published in numerous periodicals, and is also the author of books on cyber-risks and risks management. Prior to joining Willis Towers Watson, Laure held a variety of roles with insurers CNA Hardy and Nassau as well as experience in the broking industry (Aon and Gras Savoye Willis Towers Watson). □

Build Resilience.
Be Security First.

A resilient business leads with a security-first mindset to protect its data, people, and customers. With LogRhythm, your security team can:

- Manage security risk and compliance in one place
- Mature its security posture in both on-premise and cloud environments
- Automate workflows and improve operational costs
- Measurably reduce its time to detect and respond to threats
- Secure a remote workforce across disparate systems

Together, we can make the world a safer place.

Visit logrhythm.com

LogRhythm®

Cybersecurity in financial services

Compliance and reducing complexity with automation.

Businesses in the financial services sector have to manage enormous risk, wealth and personally identifiable information (PII), all while meeting strict regulatory requirements. With pressure mounting on compliance and data protection, financial services organisations are becoming increasingly motivated to improve their cybersecurity preparation, response and resilience across the sector.

According to Allianz's 'Financial Services – Risk Trends' report, attacks against the financial sector increased 238% globally from the beginning of February 2020 to the end of April, with 80% of financial institutions reporting an increase in cyber-attacks. Organisations within the sector are connected with brokers, fund managers, insurers and lenders. Combined, these factors make financial services organisations a prime target for cybercrime.

Ransomware, Distributed Denial of Service (DDoS) and phishing attacks remain the most common threats for financial services, but the methods in the threat landscape are evolving. Suppliers and partners are being used by attackers in a new method of 'island hopping', attackers infiltrate the route into an organisation by disguising themselves as a trusted source. Research by Carbon Black, shows that 33% of financial institutions have experienced a form of island hopping in the past 12 months. Watering hole attacks and Ransom DDoS are other common evolving threats.

As the proliferation of financial data continues to grow, organisations face the task of continuously protecting that information and keeping it secure, while maintaining a reputation in the financial sector. Despite this, many security teams lack the resources and funding to keep up with the evolving threat landscape and ecosystem of regulatory compliance rules.

The complexity of complying

For financial services organisations, cybersecurity is about minimising risk for both the customers and the business. This includes compliance, it is vital financial services organisations reduce the possibility of further fines or other penalties by implementing the correct security and data protection measures in the event of a breach, for example GDPR. However, this is a complex and expensive process that many businesses find challenging.

There is a growing requirement for organisations in the financial sector to detect and respond to weaknesses in authorisations that could put banks, payment transfer systems and financial data at risk. However, security teams often lack the resources to flag these rapidly, resulting in detrimental impact to multiple parties.

On top of this, Security Operation Centre (SOC) teams are often attempting to mitigate threats manually, increasing effort and stress. Security teams need to eliminate the time spent writing scripts, building rules and creating reports to allow more focus to be on evolving attacks.

Automating processes for financial security

Harnessing the correct tools and improving capabilities is becoming essential with the evolving threat landscape and new technologies that transfer, process, store, and interact with financial data.

Security teams need a proactive strategy to provide holistic visibility into their networks and improve detection and response capabilities. By addressing cybersecurity regulations with a preconfigured compliance automation software, security and data protection compliance rules are simplified into a single process.

LogRhythm reports

Attacks against the financial sector

increased 238%

globally from the beginning of February 2020 to the end of April

The compliance environment can only extend further, with more regulatory requirements coming into play. Security teams need to act now, to ensure a standard model is in place that will allow them to grow with this expansion.

80%

of financial institutions report an increase in cyberattacks

Implementing prebuilt content that is specifically mapped to the individual controls of each regulation enables instant results that do the heavy lifting for you. This type of system can help SOC teams stay on top of financial data safely while quickly navigating threats and intrusions across endpoints.

Utilising the right software will allow security teams to detect compliance violations automatically, with real-time visibility, which can deliver higher productivity, reliability, availability, increased performance, and reduced operating costs.

Combining compliance automation software with a Security Information and Event Management (SIEM) gives security teams the resources to comply with necessary mandates more efficiently and effectively than previous manual processes. A SIEM platform can facilitate security teams to improve detection, mitigation and response capabilities.

Furthermore, automation systems allow workflows to be more streamlined to help security teams combat evolving threats by removing manual tasks and enriching data with contextual details consistently.

An expanding compliance environment

Looking forward, the financial sector is expected to face continued vulnerabilities in its technological offerings, both online and traditional brick and mortar. Organisations are expected to centralise fraud and risk operations to increase visibility and detection capabilities. With compliance automation systems at the forefront of SOC teams, patterns of fraudulent activity will be detected at a greater rate, increasing the likelihood of mitigation before impact.

The compliance environment can only extend further, with more regulatory requirements coming into play. Security teams need to act now, to ensure a standard model is in place that will allow them to grow with this expansion. Financial organisations should be prepared for stricter security rules becoming a necessity to protecting both customer and business data. □

What is your IT risk assessment costing you?

The IT risk assessment process is the most tried and true method to collect and aggregate risk insights across the business. But adopting or supporting the process with technology advancements has been slow on the uptake.

Most organisations are too busy responding to and initiating action to stay ahead of risk and compliance that they do not have the opportunity to evaluate, is there a better way? IT risk assessments are a critical piece of your risk management programme. Still, the manual nature of spreadsheets and email could be holding your organisation back and even costing you resources that the business can apply elsewhere.

Problem #1 Data collection process

- *A multi-step process with opportunity for delayed completion:* Distributing IT risk assessments and coordinating between risk management and your line of business.
- *Collecting input and confirming answers across stakeholders:* A single person may not have the information for an entire assessment, but they still receive the full questionnaire.
- *The time it takes the respondent to review,* address, and complete all relevant questions.

Problem #2 Response quality

- *Answers may not match the intended inquiry:* Often assessment questions are very pointed without a lot of explanation or insight for the respondent to achieve a clear understanding.
- *Hindsight perspective:* Point-in-time responses and the lag in logging static pieces of data quickly age of scope to measure your 'current' exposure.

Watch the webinar: *10 Essential Steps to Rethinking Risk Assessments*

Time is money: Calculating your IT risk assessment resources

Risk managers build out elaborate spreadsheet-based questionnaires to collect insights from the business line about day-to-day operations and gauge what risk may be exposed. Risk assessments cover a breadth of scenarios and therefore tend to be quite lengthy. To tailor every spreadsheet to the respondent's domain knowledge would not only take more initial time but if you're managing a spreadsheet or strictly table format – it would only create additional efforts to correlate the fields across IT risk assessment variations.

- How much time do you spend creating an assessment?
- How long does it take your organisation to receive the completed assessment?
- What is the age of the data at this point?
- What time spent following up on outstanding assessments?
- How often do you need to follow up with stakeholders for clarification or explain their responses?

A traditional risk assessment process will take about...

- One week to design the assessment or confirm the scope within the second line.
- One day per risk owner to review and complete.
- One week to check answers and analyse associated risk.
- Three+ weeks to evaluate and treat risk.

This timeline does not account for extended delays in completion or follow-up to clarify or collect additional information from respondents or related business stakeholders. The extra manual efforts and hours add up on their own for your risk managers and line of business risk owners without considering additional delays.

The average salary for risk manager in Atlanta, Georgia is $112,565 according to Salary.com. Amounting to about ~$431 per day

- One week design: $2,156
- One day to respond: $431 (single risk owner)
- One week to analyse: $2,156
- Three weeks to evaluate and treat: $6,468

Based on the groundwork and execution of a single IT risk assessment in this simplified example, this can cost up to $11,211.

Spreadsheets are an asset for many businesses because they are readily available, provide flexible structure, and have a decent level of familiarity across the company. While spreadsheets have been the most uncomplicated option traditionally, that is no longer the case. Organisations need to rethink how they execute risk assessments using a modern-day platform rather than the traditional 'ease' of execution in spreadsheets.

"By leveraging OneTrust, ClearDATA saves 3,000+ minutes (over 50 hours!) a year by automating this assessment process."

Jonathan Slaughter, Director of Compliance, Security, and Privacy, ClearDATA

The real costs of IT risk assessments can be quite high and resource intensive. Risk leaders must be able to streamline this process to enhance the quality of responses and gain additional efficiencies using dedicated assessment technology and automation. IT risk assessments today should be dynamic and responsive to present the most relative information to designated stakeholders. □

OneTrust GRC reports

Are you ready for risk quantification?

This decision tree to understand if you're ready for risk quantification today – or if not – what actions can you take to enhance insights today that will support risk quantification in the future!

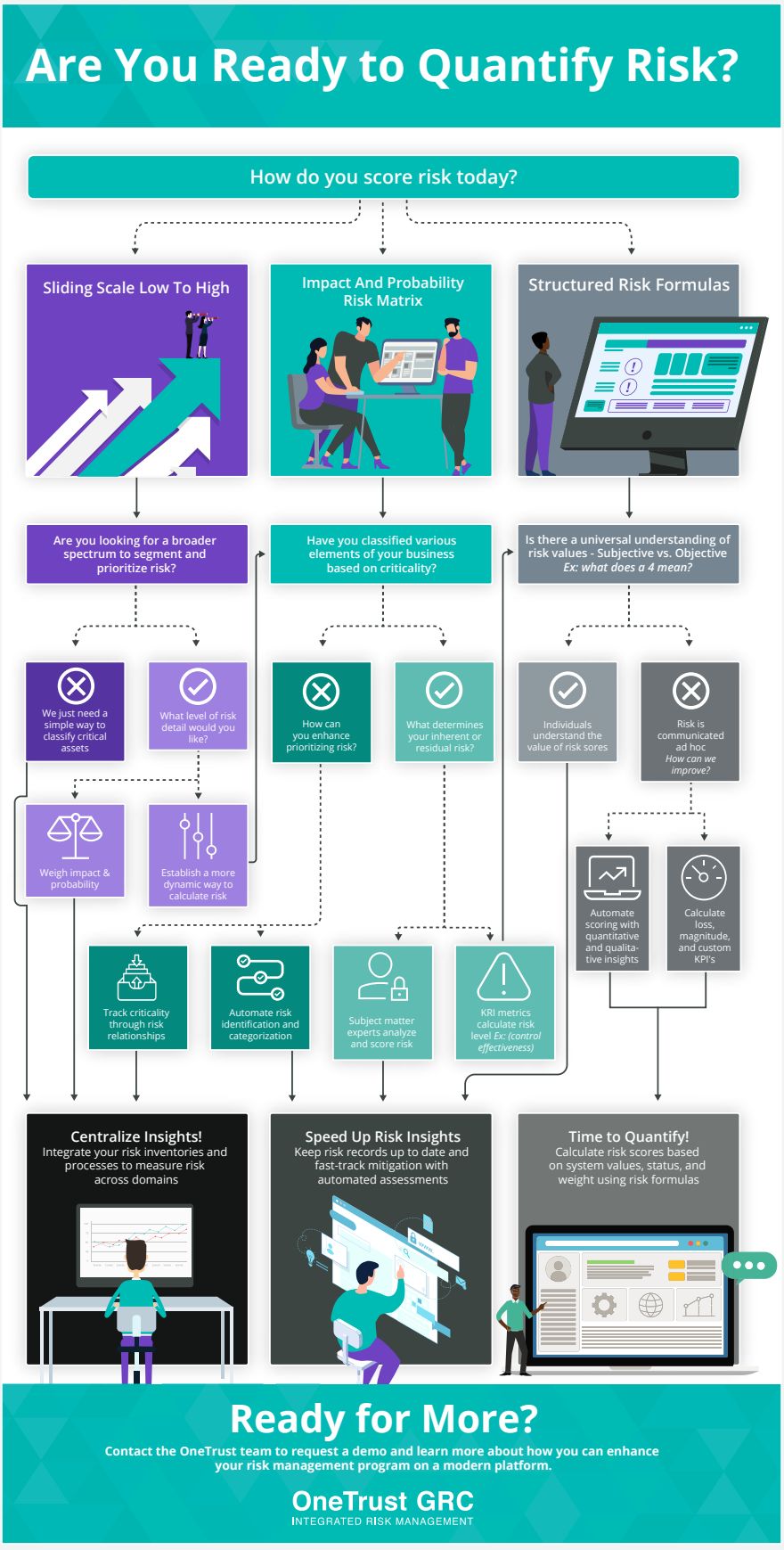
- Identify how you score risk today
- Qualify what your immediate goals are
- Realise tactics that you can leverage now

Forrester's 2021 Predictions outline an uptick in the requirements for businesses and audit professionals to quantify risk. "Risk quantification solutions that provide insights into the criticality of assets and potential impact of an issue in real-time with business context will help security leaders determine what stays, what goes, and where limited increases should go. Examine risk quantification solutions – and their substantial required dependencies – to move beyond the tried-and-true basic business case that was sufficient during the growth years."

Risk quantification can help your organisation go beyond traditional risk matrix scoring, applying values to contributing factors of risk – and calculating them across what can be massive data loads to help you gain risk insight on the risk posture of your organisation.

But for many organisations, executing a risk quantification exercise can be a resource-intensive exercise, that may or may not scale or provide the insightful ROI expected. Robust statistical models certainly have valid uses – and can help identify a dollar amount to communicate to your board or leadership. They can be a massive initiative to first get off the ground and secondly scale and maintain across various aspects of your business. At the end of the day, the inputs can still be prone to a subjective perspective. But risk quantification doesn't have to be a heavily complicated exercise – you can jump into risk quantification without jumping into the deep waters of complex statistical models.

This infographic will help you understand where you are in evaluating if your organisation is ready for risk quantification and what you can action today! □



For more information, please visit
www.onetrust.com/solutions/grc/

OneTrust GRC
INTEGRATED RISK MANAGEMENT

OneTrust GRC

INTEGRATED RISK MANAGEMENT

Enhance Visibility Across Your Business Analyze Risk, Reinforce Governance, and Scale Compliance

- IT Security Risk Management
- Enterprise & Operational Risk Management
- Incident Management
- Vendor Risk Management
- Policy Management
- Business Continuity Management
- Ethics & Compliance
- Audit Management
- Awareness Training

Have a specific area of interest? Visit the OneTrust GRC virtual booth and have a coffee and chat with the team

Corporate defence is the new black

Why value preservation should be every business' imperative.

Red Sift reports

Olde worlde

Executive-level managers (C-suite) have long understood the importance of value creation, prioritising it and explicitly addressing it at a strategic level as part of the firm's mission statement and business model.

Beyond the boardroom, shareholders, investors, and even the courts expect that directors exercising reasonable care, skill and diligence will promote the success of the company. These are principles that are considered so fundamental to business objectives that they are codified in law in Ireland, England and Wales. In the United States, directors duties are codified at State level, obliging directors to meet standards in pursuit of a businesses overarching goal, that is to *make* money.

Globally, principles of corporate governance explicitly refer to terms such as 'value creation' (King IV Report on Corporate Governance in South Africa 2016) and 'sustainable, long-term value creation' (Klaus Schwab, World Economic Forum Davos Manifesto 2020).

New paradigm

When corporate governance and indeed these principles were conceived, the world was not watching firms under daily attack from the leading significant cyber-threats: business email compromise (BEC), ransomware, and supply chain compromise.

It is well known and understood that the price of carrying out cybercrime is low; both in terms of actual costs to be met and the skill level required. Nation-state actors, organised crime gangs and lone-wolf noobs no longer need to be able to code.

New tools

These bad actors are able to access malware-as-a-service and frequently act with impunity shielded by rogue governments with scant regard for the rule of law. In fact, in some jurisdictions these governments pursue a policy of disruption and disinformation and not only tolerate but promote the pursuit of chaos beyond their borders.

It is not hyperbole to suggest that businesses and entities in the West are under constant cyber-attack to fuel and fund the activities of those intent on destabilising our way of life.

Corporate defence is the new black

Given this world and these new tools, it is incumbent upon corporate leaders to revisit their mission statement and revise their objectives to address this new reality. Firms must preserve, protect and defend stakeholder value. The world has changed and those who change with it will thrive. Rules and principles that guided us 40 years ago are no longer fit for purpose. They overlook the new reality.

It might be difficult to conceive what this means in the abstract. Helpfully, in the last three months we have seen three entities preserve value by refusing to engage with cybercriminals and pay the ransom demanded.

They are:

- The Washington D.C. Police Department (Washington D.C. PD) – United States
- Health Service Executive (HSE) – Ireland
- Bose – United States

Only Bose, the home entertainment business, had adequate back ups and sufficient resilience to avoid business disruption. Because of sound cyber-defence, Bose were in a stronger position when compared with either the Washington D.C. PD and the HSE, neither of whom appear to have back-ups. That said, neither entity compounded their initial error (weak cybersecurity) by caving to the demands of cybercriminals. Being hit with ransomware is one problem for the firm, paying the ransom demand is another.

Conclusion

In today's world, corporate cyber-defence is synonymous with value preservation. In fact, as long as value preservation is not elevated and called out as a primary corporate objective, this strategic imbalance will result in losses, whether direct or indirect.

In practice, there is no escaping the fact that failing to elevate corporate defence (i.e. adequate security, effective controls, sound risk management, sufficient resilience and so on) to a primary strategic imperative addressed at an executive level will likely lead to a permanent diminution in stakeholder value or worse. The price of continuing to do business in today's age is eternal vigilance and a robust corporate defence strategy to preserve the firm's value. □

For more information, please visit
redsift.com

RED SIFT

RED SIFT

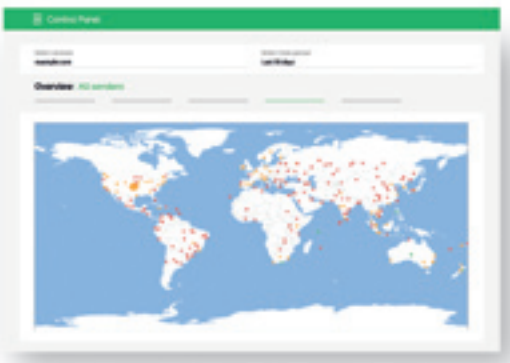
It's **400x more expensive** to stop a cyber attack than it is to start one.

We exist to **change** that.

Red Sift delivers **scalable inbound** and **outbound** email protection for less than you think.

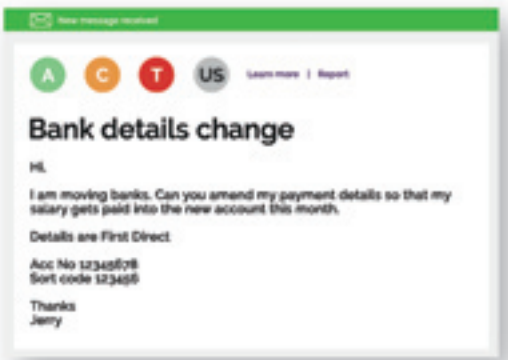
ONDMARC

Protect your domain from email impersonation



ONINBOX

Intelligent email threat detection



Trusted by: Telefónica WISE pipedrive itv Cambium Networks

Email a member of the team to find out more about our cybersecurity solutions | contact@redsift.com

5 myths about cloud migrations, debunked

For all the reasons companies decide to move to the cloud, there are just as many reasons why companies hesitate to take this important step. While some are valid, there are a lot of myths...

Virtru reports

#1: I have more control over my data on-premise

This is not always true. Many on-premise systems can leave you more vulnerable to cyber-attacks. The recent Microsoft Exchange Server attack demonstrates that hosting email, files, and data lakes on-premise can actually be a liability – these attacks began in January 2021 yet patches weren't deployed until early March.

Companies that store data in the cloud, with additional layers of security like Virtru's data encryption solutions, can take immediate action in the face of a cyber-attack or threat. By managing encryption keys and their associated policies using a distributed architecture, you can rotate encryption keys and mitigate damage right away.

The future is cloud-based – software giants are no longer investing in on-premise solutions. A fully on-premise tech stack for managing the entirety of a company's data isn't sustainable – at the very least, it can hold organisations back from becoming agile and innovative.

#2: The cloud is not secure enough for highly regulated industries

Highly regulated organisations such as financial services are moving to the cloud at a rapid pace. However, 'off the shelf' cloud solutions alone are not secure enough. With Virtru's encryption as an added layer of protection, you can unlock all the benefits of the cloud while still safeguarding your data.

Whether using cloud-based email and collaboration tools, storing a data lake in the cloud, or leveraging cloud-based apps like Salesforce, Zendesk or SAP, Virtru's encryption solutions can be layered in for greater security, so many of the strictest compliance regulations can still be met.

#3: We can't maintain data sovereignty while using a US-based cloud provider

Data sovereignty refers to the idea that data is subject to the laws and regulations of the geographic location where it is collected and processed. Many companies are hesitant to move to cloud platforms like Amazon, Google, and Microsoft, out of concern that they will not be able to maintain true ownership over their data.

However, US cloud providers now account for 66% of the European market and companies don't have to sacrifice true ownership of their data for the benefits of the cloud.

Virtru's end-to-end encryption solutions satisfy data sovereignty requirements by protecting sensitive data at the time of creation and providing the ability to store encryption keys in their required geographic region while allowing the organisation to continue using the multinational cloud vendor of their choice.

#4: Moving to the cloud is cost prohibitive

While there is an upfront cost to cloud migration, it can alleviate costs over time. Companies can eliminate redundancies, streamline their technology stack, and increase flexibility and speed to market. And often it is the business technology strategy that drives the overall strategy and growth for an organisation – as highlighted in a recent survey by Deloitte and WSJ Intelligence, 40% of CEOs said that CIOs would be the key driver of business strategy in the next three to five years.

Many large organisations are saddled with technical debt, which can also delay cloud migrations. Ensure your organisation is looking at a long-term strategy for lessening the burden and cost of legacy technology that are no longer serving your business.

#5: My staff can't support a cloud environment.

A recent Virtru adopter shared his advice for cloud migrations: "Invest in making experts out of a select group of people in your organisation and get them to share their knowledge. People respond better to training from peers and your trainers will have an intimate knowledge of the organisation, which really helps when rolling out the new systems."

The truth is that no one knows your data better than your own employees. By ensuring alignment with internal teams, you may discover important requirements that will impact your overall cloud strategy.

Moving to the cloud can unleash greater productivity, data sharing, and innovation for your organisation – and for many companies, file and email encryption (with self-hosted keys) can be a game changer. To learn how Virtru can enable your cloud migration, contact us today. □

Your Keys to the Cloud.

With Virtru, **only you** hold the keys to your data in the cloud, so no one—not even your cloud provider—can access your protected data without your permission.

Virtru's end-to-end data protection enables you to store and share even the most sensitive information in the cloud, while remaining fully under your control at all times.

See how Virtru's data-centric encryption can enable secure data sharing in the cloud. Start the conversation today: **virtru.com/contact-us**

virtru

How integrated data loss prevention solutions help financial firms improve their email security

Empower staff with data protection tools they'll actually want to use.

Zivver reports

With email still the main business communication tool worldwide and new channels frequently coming online, more information is being shared digitally than ever before, creating fresh security challenges. But safeguarding data goes beyond strong encryption and defending against cyber-attacks, companies must also look closely at their email data protection.

Many financial sector companies believe they already have a solution in place that offers email data protection, but usually this only solves part of the puzzle and is often designed to provide a sub-optimal experience for your staff and message recipients. This in turn puts financial data and PII at increased risk, which makes the situation far from ideal.

What type of security risks do we mean? Accidental data leaks from staff.

Security incident reports, including from the ICO, routinely show that **most data leaks occur before employees send information**, specifically caused by:

- Auto completion functionalities of email clients, accidently adding the wrong recipient
- Attaching a file that contains sensitive information the user is unaware of
- Users not being aware that the information they're sharing is sensitive
- Exposing recipients contact details by failing to use 'Bcc'

Practically everyone has made a mistake like that before, sometimes it's embarrassing and relatively harmless, other times it can be highly consequential and cause lasting reputational damage.

But let's face it. **When a security tool isn't intuitive or simple to use, the adoption of it will be low and slow.** This makes it more challenging to ensure that data remains protected, and that staff are communicating in a safe and compliant way. **Which leads to an important question: if your staff won't bother using the tool, what's the point of having it?**

The most effective DLP solutions should easily integrate with your company's way of working, and be simple for staff as well as recipients to use. This is done by adding a security layer on top of your existing email (or other systems such as Salesforce), which means there's no need for employees to change workflows and they can work in an environment they're already familiar with.

Zivver's human layer email security solution helps over 4,000 companies, including global financial firms, achieve the following:

- *Prevent data loss caused by insider threats:* Zivver integrates seamlessly with popular email clients (Outlook, Gmail, OWA) to raise employee awareness when handling sensitive data. Real time alerts prevent data leaks, and staff can recall an email if a mistake happens.
- *Fill the outbound security gaps found in existing email and cybersecurity platforms:* Zivver offers an enhanced level of security using asymmetric zero access encryption, preventing any type of unauthorised third-party access.
- *Save time and money:* reduce unnecessary spend on paper, print, and postage, communication and sharing tools, plus awareness training. Companies using Zivver have saved millions per year from these cost reductions!
- *Enhance client satisfaction by minimising the use of portals or user accounts:* having more efficient ways of communicating with customers leads to better service, higher NPS, a competitive advantage, and more time to spend on your core business.

At Zivver, we believe that **employees are not risks to be mitigated, but are key assets to be enabled**. When people are equipped with the right digital tools and understand how their behaviour impacts the frontline of email security, they become much more efficient at detecting scams, preventing data breaches, and protecting sensitive information. □

zivver

A human layer email security solution that:

Prevents data loss
caused by insider threats

Fills the outbound security gaps
found in existing email and cybersecurity platforms

Saves time and money
from paper based processes

Enhances user satisfaction
reducing cumbersome account and portal issues

"Zivver saves 10 minutes per sent offer instead of using the postal services. And with our daily offer rate, we save hours each day!"

Paratus - Foundation Home Loans

Book a demo today **zivver.com**

Multicloud security: more clouds, more problems

Today, cloud vendor lock-in fears of the past seem overblown. Instead of choosing one cloud or another, organisations are simply choosing both, or to be more precise, many!

BeyondTrust reports

Most organisations aren't merely in the cloud – they're in many clouds (PaaS, IaaS), and their end users regularly consume dozens, or even hundreds, of different SaaS applications. A McAfee study published in 2019 reported the average organisation used 1,935 cloud services. And that number has almost certainly ballooned further since then.

Over the past year, the great cloud migration has enabled the successes of increased remote working and is propelling the acceleration of digital transformation initiatives. Yet, more clouds can mean more security and operational challenges. Siloed identity stores (i.e. Azure ID), native, but incomplete toolsets, and conflicting shared responsibility models between cloud providers – along with all the fundamental cloud security challenges – is creating a fertile atmosphere for threat actors. Additionally, most companies are not 100% cloud – they operate with a hybrid model that includes an on-premises infrastructure, often based on legacy technology.

Inadequate privileged access security controls – often involving credentials, excessive privileged access, or misconfigurations – play a role in most breaches today across both cloud and on-premises environments. The scale of managing the exploding universe of privileges requires an integrated, universal approach, rather than relying on a stack of niche tools, each only helping to manage a slice of the privilege problem. This is especially true when the elasticity of the cloud allows for rapid changes that even traditional tools for management and governance may miss.

Many organisations already run at high risk from over-privileged IT administrators and power users. As they migrate more workloads to the cloud, the on-premises complexity doesn't vanish. Instead, they tend to end up with the hybrid, multicloud management challenge.

Lean into identity-centric security to address the most critical multicloud and hybrid IT security gaps

As environments have trended toward increasing decentralisation, identity has become the strongest foundation for security. The identity challenge is the most important security problem for organisations to solve for across cloud and on-premises environments. And no identities are more critical to protect than privileged identities – whether associated with humans or machines, employees or vendors, and whether they are persistent or ephemeral. Solving for the multicloud/hybrid identity and privilege challenges is best accomplished by standardising the management and security controls across the entire IT ecosystem.

Ultimately, your privileged access management strategy should ensure every privileged account, session, and asset is secured, managed, and monitored across your entire cloud and hybrid infrastructure. BeyondTrust Privileged Access Management (PAM) solutions protect your entire multicloud and hybrid environment via our universal privilege management model by:

- Continuously discovering and onboarding privileged accounts and cloud instances
- Enforcing credential security best practices across every human and non-human account, including implementing zero trust architectures
- Reducing the number of users with privileged access
- Restricting the privileges any user, application, service, or asset has for access and automation
- Preventing and mitigating human-based errors in privileged access
- Condensing the window of time during which privileges can be executed, and thereby abused, by applying the principle of just-in-time access
- Enforcing segmentation of the cloud environment and securing/proxying remote access to cloud management consoles/control planes and to computing resources
- Robustly managing and monitoring every privileged session and providing certification for regulatory compliance
- Providing a single, centralised platform for all privilege management activity that is architected to integrate with the rest of your security and information technology ecosystem

For a deeper dive on understanding and addressing the most pressing multicloud security risks and challenges, download our new Guide to Multicloud Privilege Management. □

For more information, please visit
www.beyondtrust.com

BeyondTrust

BeyondTrust

UNIVERSAL PRIVILEGE MANAGEMENT

Secure and protect privileges across passwords, access, and endpoints to stop data breaches and achieve compliance

Privileged Password Management

Endpoint Privilege Management

Secure Remote Access

beyondtrust.com

The only universal security intelligence solution

Recorded Future – delivering relevant cyber-threat insights in real time.

Recorded Future reports

Who we are

Using a sophisticated combination of machine and human analysis, Recorded Future fuses the broadest set of open source, dark web, technical sources, and original research together to deliver relevant cyber-threat insights in real time. The Recorded Future Security Intelligence Platform aggregates this rich intelligence with any other threat data sources, which empowers security teams to collaborate on analysis and deliver intelligence wherever they need it most – including rapid integration with existing security solutions.

Security intelligence solutions

Security intelligence accelerates detection, decision-making, and response times by positioning comprehensive intelligence at the centre of your security workflows.

- *Threat intelligence:* Gain context on who is attacking you, their motivations and capabilities, and indicators of compromise to look for in your systems. This information is searchable in real time and presented in a single-pane-of-glass view and via customised alerts.
- *SecOps and response:* Discover previously unidentified threats and triage internal alerts in your SIEM based on rich external context and threat indicators correlated with internal threat data – so you can make faster, more confident decisions
- *Brand protection:* With real-time alerting, you can find things like leaked credentials, typosquat domains, social media accounts meant to impersonate an employee or brand, fake applications, threats to executives, and more. Takedown services go the last mile to simplify and expedite the removal of malicious content from the internet.
- *Vulnerability management:* Real-time risk scores based on real-life exploitability make it easy to prioritise where you should focus efforts and what you need to patch to prevent attacks. Real-time alerting on vulnerabilities affecting your tech stack provides new insights for effective risk reduction.
- *Third-party risk:* Make informed decisions to reduce your overall risk based on insights from real-time intelligence about the vendors and partner companies that form your business ecosystem – including vulnerable technologies, domain abuse, threats targeting the organisation, and more.

Intelligence-led security

Lead with intelligence across your security teams, processes, and workflows with security intelligence solutions from Recorded Future.

- Threat intelligence
- SecOps and response
- Brand protection
- Vulnerability management
- Third-party risk
- Geopolitical risk

- *Geopolitical risk:* Accelerate critical decision making with contextual data on threats, trends, sentiments, and evolving security situations – so you can protect your assets and understand shifting geopolitical dynamics in the geographic areas that matter to your organisation.

Innovative security intelligence technologies

Security Intelligence Graph

Recorded Future's unique ability to model all relevant security information available on the internet is what has set us apart since the beginning. With billions of indexed facts, and more added every day, the Recorded Future Security Intelligence Graph leverages a unique combination of patented machine learning and human analysis to provide you with unmatched insight into emerging threats that are relevant to your organisation.

Recorded Future Intelligence Cards™

Security teams gain instant context around suspicious observables and indicators with Recorded Future Intelligence Cards – with just one click. This innovation enables security teams to rapidly prioritise threats or dismiss false-positives using Recorded Future's dynamic risk scores. All of the evidence gathered by our Security Intelligence Graph is visible on these cards, allowing you to pivot quickly between indicators and attack methods, or vulnerabilities and exploits. □

For more information, please visit
www.recordedfuture.com

Recorded Future®

Privileged access management challenges when moving to the cloud

Cyber-attackers are capitalising on accelerated cloud transformation.

Jason Mitchell reports

The move to broad-based remote work has accelerated many organisations business requirements to move more infrastructure and services into the cloud. Gartner estimates that 80% of organisations are predicted to migrate toward cloud, hosting, and colocation services by 2025, and new attack surfaces will arise and create greater security vulnerabilities.

However, our research showed that between March 2020 and March 2021, 65% of organisations saw attempted attacks on their cloud environments, with 80% being successfully compromised.

The cloud has emerged as a considerable expansion of the attack surface, and has added new complexities that organisations are still adapting to outside of on-premises data centres. Cyber-attackers have taken notice, and are capitalising on accelerated cloud transformation where security may not get the time or attention needed to be effective.

This is especially troublesome when it comes to privileged access. The same survey revealed that 90% of cyber-attacks on these cloud environments involved compromised privileged credentials. Cybercriminals are going after the 'keys to the kingdom' to get as much access as possible, find data to compromise, and profit off their devious deeds.

What are some of the complexities that the cloud and other transformative technologies are introducing to IT environments? Cloud workloads are no longer just being accessed by humans, but access can also be requested by machines, services, APIs, and more. Credentials and entitlement enforcement has gone from using shared accounts to now using individual identities for more accountability. The control posture can no longer be static, but must be dynamic, AI-driven, and risk-aware.

When it comes to the cloud, specifically, one big challenge is that different groups inside the organisation will have their own requirements. The needs of the infrastructure and compliance teams are going to be much different to those of the engineering and development teams, the security and identity teams, or even the cloud architecture teams.

For example, identity sprawl can be a huge challenge when moving to the cloud. For each cloud provider you add into the mix, you're going to need a way to authenticate users to access those workloads. This can mean spinning up a completely new set of identities, which all need to be managed including their privileges and entitlements.

Some teams will say that's fine, or they will want all of the credentials to be stored in a password vault. But that doesn't solve the management challenges, or ensure compliance and accountability. This becomes increasingly relevant once organisations start using multiple cloud providers.

One way to solve this challenge is with a multi-directory brokering solution, where all identities' entitlements and privileges are still kept in the main identity repository of choice, and then access privileges are brokered out to cloud providers and workloads.

When combined with multi-factor authentication and federated access without exposing the password, this solution presents an optimised, secure, and productive method of ensuring only the right identities get access to the cloud workloads they are allowed to.

Furthermore, by basing privileged access on each individual identity, least privilege access controls can enforce just enough access, just-in-time, for long enough to get the job done. Then the access rights are removed, leaving zero standing privileges and closing potential exposure points.

To fully benefit from rapid technological transformation, it is imperative that enterprises embrace strategies for safeguarding their infrastructure and services both during and after cloud migration. Managing a secure transformation to the cloud can be much smoother by centralising identities, leveraging existing technology, simplifying complexity whenever possible, and always enforcing a least privilege approach to identity and access controls. □

Jason Mitchell is SVP, Engineering at Centrify.

For more information, please visit **www.centrify.com**

Centrify

Improve the Security and Compliance Posture with Centrify Privileged Access Management

Trusted by top banks and financial institutions, Centrify Privileged Access Management solutions help tackle the #1 cause of today's breaches — privileged access abuse.

#Centrify, has you covered when it comes to securing your ever-expanding attack surface against privileged access abuse — be it by insiders or external actors. In addition, Centrify Privileged Access Management solutions establish continuous visibility into compliance, for key regulations such as Sarbanes-Oxley (SOX), PCI DSS, MAS, Gramm-Leach Bliley (GBA), NYS DFS, or GDPR.

Ready to protect against the #1 attack vector? Contact us to minimize your attack surface and control privileged access to your hybrid environment. **www.centrify.com**

Connect with us on social!

Online work is now your safe space.

Menlo Security eliminates threats from Malware, fully protecting productivity with a one-of-a-kind, isolation-powered cloud security platform.

MENLO SECURITY

Learn how at menlosecurity.com/why

Why SASE is primed to secure the evolution of finserv

Finserv is an industry leading the charge when it comes to the digitisation of services, yet, despite the consolidation of hybrid and remote working models, a degree of scepticism remains over networking alterations owing to the vital importance of industry security. Here we explore SASE as a means of enhancing productivity while maintaining a security-first approach.

Tom McVey reports

Few industries have changed as dramatically as financial services (finserv) in the last decade.

Where banking and financial transactions were once exclusively an in-person and largely paper-based process, the vast majority of financial affairs are today managed digitally, with a variety of new innovations and services powering an ever-advancing market.

Be it fintechs, challenger banks, blockchain, mobile banking solutions and more, finserv today looks unrecognisable compared to the industry that existed even a mere half decade ago.

The improvement of service forms just one element of the industry's innovative focus, however. Behind the scenes, banks, credit unions, insurance firms, mortgage companies and others have been working to transform their own infrastructure to streamline processes, optimise productivity, enhance security, and operate in a more effective, agile, and flexible manner.

COVID-19 needs little by way of introduction. Much like many industries, finserv was flipped on its head by the pandemic back in early 2020.

Where industry players had primarily operated out of offices, social distancing restrictions and enforced national lockdowns shifted the hub of productivity to the home, with organisations having to adapt to such dramatic overhauls in a matter of days.

From an IT perspective, it presented a challenge. Where many felt the pandemic may have lasted a matter of weeks and a necessity for home working was therefore a temporary fixture, VPNs were implemented to provide disparate employees access to key resources and applications by tapping into on-prem network infrastructure.

18 months on, however, it's safe to say that flexible, remote and hybrid operating models are – at least in part – here to stay. With this in mind, it is time for organisations to consider how they might uphold such models more effectively moving forward.

Why SASE?

Yes, VPNs initially made sense, acting as an extension of a company's on-premise IT infrastructure. Yet they are equally fraught with challenges, and are simply not a viable, productive long-term solution.

While VPNs are capable of connecting employees in disparate locations to a centralised on-premises network, these very same networks were not designed to support remote operations. As a result, they can lead to bottlenecked traffic, hampered productivity and security vulnerabilities where network managers are forced to make visibility concessions.

With employees now located across varied locations, as are many of the cloud-based tools and applications they use to complete their work effectively, the question is why would their network need to be managed and secured from a centralised, on-premise location that is no longer being physically used?

Finserv should instead shift this activity to where the work is now happening – in the cloud. In doing so, a variety of benefits can be realised.

Visibility can be increased using products like CASB, DLP and Secure Gateway, while bottlenecked traffic and friction with users will be eliminated without the need for them to jump through intricate, laborious, sub-optimal hoops to access vital tools and data.

Here lies the argument for Secure Access Service Edge (SASE) adoption.

Coined by Gartner, SASE entails the simplification of a company's networking and security functions by interlinking both elements as a cloud service that acts as an extension of the user, bypassing the need for an enterprise data centre.

SASE is not a single solution. Rather, it is a concept comprising the amalgamation of pre-existing software-defined wide networking (SD-WAN) capabilities and network security functions (such as

Unlike legacy solutions and the use of 'square-peg-round-hole' VPNs, SASE has been built with a cloud-first mindset. As a result, it is able to provide complete, seamless protection and visibility, while equally prioritising productivity.

CASB, Cloud SWG, ZTNA/VPN, WAAPaaS, FWaaS, DNS, RBI and other relevant components).

The key thing is that SASE is not a case of revolutionising security. Rather, it is a natural evolution that uses the same techniques used by on-prem infrastructure in the cloud.

Unlike legacy solutions and the use of 'square-peg-round-hole' VPNs, SASE has been built with a cloud-first mindset. As a result, it is able to provide complete, seamless protection and visibility, while equally prioritising productivity.

Indeed, SASE is garnering significant attention at present as an IT framework that is much better suited to supporting today's dynamic secure access needs. Yet as a relatively novel concept, there is naturally some hesitancy as to its effectiveness, particularly within highly sensitive circles such as finserv.

While legacy security solutions are arguably outdated in terms of their usability, they are extremely secure. The question, therefore, is whether SASE can match these standards.

Zero Trust is key

In order for it to achieve the required levels of security, SASE should be incorporated in tandem with a Zero Trust philosophy.

Zero Trust is a natural fit for the finserv industry. The sector has historically taken a Zero Trust approach with its vital assets, having previously used bank vaults and other high-tech security investments that keep all persons out – both internally and externally of the organisation.

Isolation is one method in which Zero Trust can be achieved in a highly effective manner within a cloud network.

It is a technique that shifts the point of execution for active content away from a user's browser to a disposable, cloud-based virtual container. This essentially acts as a screen, preventing all active content including exploit code from reaching its intended target. Thus, it prevents cyber-attacks on a user's machine.

Isolation separates the enterprise network from public access while providing users with secure, low-latency connections to the vital resources and SaaS applications that they need. All content is rendered safely in a remote browser so that any potentially malicious code simply does not have an opportunity to execute on the end point.

It is not 'almost safe' like other security solutions. Rather, it can stop malware 100% of the time.

Cloud-first is inevitable

Indeed, while SASE, Zero Trust and isolation may appear to be relatively novel trends, it is important to understand that technologies such as these that have been engineered to support cloud-first models will undoubtedly become the future of networking and security.

In the case of SASE, where Gartner had originally predicted that it would take 10 years for the concept to become mainstream, the pandemic has now cut this projected timeframe in half.

Research shows that 67% of finserv firms will be looking to deploy an SD-WAN in the next year – a key component in SASE. Further, 54% of organisations are prioritising improvements of visibility and security for home infrastructure.

Despite having barely been mentioned two years ago, the technologies and ideals that underpin SASE are rapidly becoming a priority for many businesses looking to optimise their hybrid, flexible and remote business models in the new normal.

The tide is clearly turning in favour of cloud-first models. And while security hasn't always been a primary investment priority for businesses, owing to a lack of tangible return on investment, SASE is changing that narrative, with its productivity, accessibility and futureproofed characteristics capable of embedding sound security alongside a series of wider benefits. □

Tom McVey is Sales Engineer EMEA at Menlo Security.

For more information, please visit **www.menlosecurity.com**

MENLO SECURITY

Forthcoming events

SECURING THE LAW FIRM VR

16th September 2021
Online

e-crime & cybersecurity MIDDLE EAST VR

5th October 2021
Online

e-crime & cybersecurity MID-YEAR VR

14th October 2021
Online

e-crime & cybersecurity NORDICS VR

27th October 2021
Online

e-crime & cybersecurity SPAIN VR

24th November 2021
Online

e-crime & cybersecurity BENELUX VR

8th December 2021
Online

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

Thank you to all our sponsors

Strategic Sponsors

DARKTRACE

ExtraHop

FORTINET

INTSIGHTS
Democratizing Threat Intelligence™

proofpoint.

okta

Recorded Future®

Education Seminar Sponsors

BeyondTrust

Centrify®

LogRhythm®

MENLO SECURITY

OneTrust GRC
INTEGRATED RISK MANAGEMENT

RANGEFORCE

RED SIFT

virtru

zivver