

Security

ADVISOR

MIDDLE EAST

SPECIAL:
CISO 50 &
FSA AWARDS
2021
(pg 26)

▼
**SECILORE
ROUNDTABLE**
(pg 34)

INTERVIEWS

KASPERSKY
(pg 10)

—
VERITAS
(pg 24)

DO YOU KNOW
your **BREACH**
LIKELIHOOD?

CHERIF SLEIMAN, CHIEF REVENUE OFFICER AT SAFE SECURITY, TELLS ANITA JOSEPH WHY KNOWING IS CRITICAL TO BUILD A SAFER DIGITAL FUTURE. A SECURITY ADVISOR EXCLUSIVE. (pg 14).

Experience the **POWER** and **CONVENIENCE** of AI POWERED Wi-Fi

D-Link®

EAGLE PRO AI

One Connection - Infinite Possibilities



AI Mesh Optimizer



AI Wi-Fi Optimizer



AI Parental Controls



AI Traffic Optimizer



AI Assistant

The EAGLE PRO AI Series brings AI-enhanced capabilities to optimize your Wi-Fi, and the AI Assistant to intelligently monitor network usage to give simple, actionable recommendations to keep your network at peak performance for everyone in the family.

EAGLE PRO AI Series

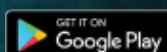


R15
ROUTER

M15
MESH ROUTER



E15
EXTENDER



EAGLE PRO AI

<https://me.dlink.com> | info.me@me.dlink.com

Connect to more...



06 **NEWS**
Top cybersecurity news snippets from the region and beyond.

10 **INTERVIEWS**
Emad Haffar, head of technical experts, META at Kaspersky, on modern-day cyber defence strategies. cyber security defenders.

24 Arthur Dell, technology leader at Veritas, on the barriers facing enterprises over cloud data protection, why SaaS has emerged as the preferred model of

adoption and how its recent acquisition of Hubstor will enhance its security offering to its customers.

26 **AWARDS ROUND-UP**
CISO 50 & FSA Awards-celebrating excellence in security leadership.

46 **FINAL WORD**
Sunil Paul, co- founder & managing director at Finesse, on how managed service providers can help, as remote work models become increasingly popular and the push towards digital transformation intensifies.

MEET THE RALLY FAMILY, FOR VIDEO MEETINGS OF ALL SIZES.



The Logitech® Rally family of all-in-one video bars and modular conference camera systems delivers the performance, installation ease, and device management tools you need to video-enable small, medium, large, and multipurpose rooms throughout the workplace.

SUPERIOR AUDIO AND VIDEO

Every Rally device features motorized pan and tilt lenses and AI-powered RightSense™ technologies for expansive room coverage with automatic framing, lifelike video quality, and exquisite voice clarity.

FLEXIBLE DEPLOYMENT OPTIONS

Available in pre-configured systems with Logitech Tap for Google Meet, Microsoft Teams®, Zoom Rooms, GoTo, Pexip, and RingCentral. Or, deploy in USB mode to use with any software.

VERSATILE SETUP AND CABLE MANAGEMENT

Find the perfect setup for any space—go modular with the expandable options of Rally Plus for larger rooms or choose the all-in-one ease of Rally Bar or Rally Bar Mini. Whichever you choose, integrated cable management keeps connections tight.

EASY TO MONITOR, MANAGE, AND SUPPORT

Get ahead of possible issues with remote device management using Logitech Sync. Monitor device status, push firmware updates, and even measure room utilization.

Raise the bar on your video meetings with Rally Family.

logitech®

EDITORIAL



Talk to us:

E-mail:

anita.joseph@cpimediagroup.com

Anita Joseph
Editor

A NEW APPROACH

Cybersecurity is at the top of every boardroom discussion today-it's amply clear that the security of virtual assets and critical data is no longer just an option. However, are the organisations doing it right? Are they spending money on the right technologies and the right approach? If experts are to be believed, the answer is NO. Studies show that while investments in cybersecurity are increasing day by day, all that money is getting wasted in unnecessary rhetoric and impractical solutions.

So, is it time for a new approach? Our exclusive cover story brings a whole new perspective into the mind-boggling world of cybersecurity by claiming that knowledge and visibility are the key to a safe and secure world. Not only that, it offers a glimpse into the new and evolving area of cyber risk quantification-a unique approach to enhancing the knowledge and visibility needed to make informed decisions. Cherif Sleiman, chief revenue officer at Safe Security, is the man of the moment-his overview of present-day cybersecurity and insights on cyber risk quantification, make for a refreshing read.

"CYBERSECURITY INVESTMENTS ARE INCREASING DAY BY DAY."

That's not all, and it gets more interesting-we have a special feature for you on the CISO 50 & Future Security Awards that CPI hosted early in September to celebrate the decision makers in the Information Technology/cybersecurity industry. The gala event, held at the Grand Habtoor Autograph Collection resort, received an overwhelming response and the award winners were all truly deserving. So, for those of you who missed the action-we bring you a sneak-peek into the glitter and glamour of the evening,

and the details of all the winners. Make sure you don't miss it!

We also have a special interview with Emad Haffar, head of technical experts, META,

Kaspersky, on modern-day cyber defence strategies and a tete-a-tete with Arthur Dell, technology leader at Veritas, to find out more about the barriers facing enterprises over cloud data protection. In addition, we have the regular news roundup, insights and opinion pieces to make your reading a thorough and enjoyable experience. So, Happy Reading!

EVENTS



FOUNDER, CPI MEDIA GROUP
Dominic De Sousa (1959-2015)

Published by

CPI

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

EDITORIAL Editor
Anita Joseph
anita.joseph@cpimediagroup.com

DESIGN Senior Designer
Analou Balbero
analou.balbero@cpimediagroup.com

Registered at
Dubai Production City, DCCA
PO Box 13700
Dubai, UAE

ADVERTISING Group Sales Director
Kausar Syed
kausar.syed@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

DIGITAL SERVICES Web Developer
Adarsh Snehanjan

Reception: +971 4 5682993
Operations: +971 4 5682994
Accounts: +971 4 5682995

Senior Sales Manager
Sabita Miranda
sabita.miranda@cpimediagroup.com

© Copyright 2021 CPI
All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

SAFE SECURITY APPOINTS CHERIF SLEIMAN AS CHIEF REVENUE OFFICER TO HEAD EMEA

CHERIF SLEIMAN,
CHIEF REVENUE
OFFICER AT SAFE
SECURITY



Safe Security, a

pioneer in Cybersecurity & Digital Business Risk Quantification has announced its entry into the EMEA region, to build on its success in North America. Headquartered in Palo Alto, California, Safe Security helps organisations manage, measure and mitigate cyber risks with its breach likelihood prediction platform SAFE. Backed by marquee investors such as British Telecom Group, John Chambers and other prominent industry leaders, the company appointed Cherif Sleiman, a veteran industry leader to head the business for international markets. Sleiman is a visionary technologist and 'turnaround specialist' who will focus on building Safe Security's regional presence, go-to-market and channel strategy in the region.

Cherif said: "Cybersecurity is a global concern. For all of the time, money, and energy spent telling us how to protect ourselves including what to buy to do so, there's little sense of actual progress when it comes to security. And that's key, because safety is not about how much money we spend on products, analysts or investments, it is simply about Knowing. Safe Security is uniquely positioned to provide organisations with the knowledge necessary to better secure their organisations. The SAFE platform delivers 360 degree continuous, dynamic & intelligent quantitative cyber risk management and breach likelihood prediction by assessing People, IT Infrastructure, Cloud Presence, SaaS Deployments and Third-Party Partnerships. It streamlines the knowledge and language needed by all stakeholders, from the boardroom to the frontline security professionals, so accurate decisions and actions can be taken in a timely fashion."

HELP AG PARTNERS WITH ZSCALER TO OFFER ZERO TRUST CLOUD-BASED SECURITY

Help AG, the cybersecurity arm of Etisalat

Digital and the region's trusted IT security advisor, has partnered with Zscaler™, leaders in cloud security. Zscaler provides enterprises with cloud security services that replace the traditional inbound and outbound gateways, helping organisations transform their network and security infrastructures from an appliance-based model to a modern, cloud-based approach.

Commenting on the partnership, Stephan Berner, CEO at Help AG, said: "Zscaler will enable us to offer our customers a zero-trust solution that securely connects any user, device, or app over any network with a revolutionary new approach to application access and security."



STEPHAN BERNER,
CHIEF EXECUTIVE
OFFICER AT HELP AG



SEAN SULLIVAN,
DIRECTOR EMEA
CHANNELS AT ZSCALER

"We're looking forward to the partnership with Help AG to accelerate their customers' secure journey to the cloud. By combining network, application and security to meet the demands of today's modern hybrid workplace, our Zero Trust Exchange Platform enables a smooth transformation journey from on premise security to the cloud," said Sean Sullivan, director, EMEA Channels at Zscaler.

ESET TO HIGHLIGHT NEW CYBER ESPIONAGE DISCOVERIES IN EASTERN EUROPE, FINANCIAL CRIME IN LATIN AMERICA AT VB2020

ESET, a global leader in IT security,

will highlight its top research for 2020 during the VB2020 localhost conference. This year, the Virus Bulletin international conference will go entirely online, thus the name change. The virtual event will take place over three days from September 30

to October 2. ESET researchers will hold four presentations and participate in one panel debate. Two notable research presentations, which have not been published before, are the discovery of knowledge sharing among Latin American financial cyber criminals and a previously undisclosed cyber espionage operation targeting several governments in Eastern Europe, the Balkans and Russia. The conference is free this year, with registration required.



ESET at the 30th
VB Conference

30 SEPT - 2 OCT, 2020

First to present will be Jakub Souček and Martin Jirkal, from ESET's R&D center in Prague, about Latin American financial cybercriminals - competitors in crime who benefit from sharing tactics, techniques and procedures.

Even though knowledge sharing among cybercriminals is not unusual, seeing so many examples of it in region-specific malware families with the same focus caught the attention of ESET researchers. The presentation will take place on October 1, 19:45-20:15 CEST.

The second presentation will cover a discovery ESET researchers made earlier this year: a previously undisclosed cyber espionage operation targeting several governments in Eastern Europe, the Balkans and Russia.

MANAGEENGINE POSITIONED IN 2021 GARTNER MAGIC QUADRANT FOR UNIFIED ENDPOINT MANAGEMENT TOOLS

ManageEngine, the enterprise IT

management division of Zoho Corporation, has announced that it has been named a Niche Player in the 2021 Gartner Magic Quadrant for Unified Endpoint Management (UEM) Tools. The recognition is based on the evaluation of ManageEngine's flagship UEM software, Desktop Central, for its ability to execute and completeness of vision. ManageEngine was included in the Magic Quadrant alongside seven other vendors.

"The need for a unified tool to manage and secure employees' devices is at an all-time high, as more and more organisations tackle a hybrid workforce fast-tracked into adoption by the pandemic," said Mathivanan Venkatachalam, vice-president of ManageEngine. "This recognition by Gartner

MATHIVANAN
VENKATACHALAM,
VICE-PRESIDENT AT
MANAGEENGINE



validates our alignment with our customers' requirements and our delivery of integrated device management and security."

"ManageEngine Desktop Central is a comprehensive tool to centralise your endpoint management across Windows, macOS and Linux machines," said an IT security manager in a Gartner Peer Insights review. "It offers operating system and third-party patch management with automation capabilities to test and deploy patches. Desktop Central provides great visibility via standard and custom reports, and great support services."

AMIVIZ INTRODUCES UNISYS STEALTH SECURITY SUITE IN MIDDLE EAST



AmiViz, the Middle East region's first

enterprise B2B marketplace has announced that Unisys Stealth suite of security solutions will now be available on its marketplace at www.amiviz.com, and that channel partners can buy the products through the web portal or the mobile app. The product range will also be available on AmiViz's Virtual Customer Experience Centre (CEC LAB). This will help resellers demonstrate to their customers the product capabilities and integration with other vendor technologies by providing a unique customer-specific environment in the cloud. Customers can request for Proof of Concept (POC) in the cloud to explore the product capabilities.

Stealth isolates cyber threats quickly and builds resilience into organisations'

environments. By partnering with Unisys, AmiViz offers its community of resellers, partners and their customers better protection of their data and infrastructure. Stealth also optimises resilience of the environment so that businesses can move from crisis to confidence, while protecting legacy systems. With this they can still function without major upgrades.

Stealth also provides organisations with "Always On" security by establishing a software-defined perimeter that enables a Zero Trust environment. Stealth reduces attack surfaces by discovering and understanding network assets and their communication flows, then creating dynamic, identity-driven microsegments called Communities of Interest, separating trusted systems, users and data from the untrusted. Encryption between endpoints cloaks assets from unauthorised users, while Dynamic Isolation™ capabilities quickly isolate devices or users at the first sign of compromise.

QAKBOT BANKING MALWARE IS ON THE RISE: NUMBER OF ATTACKED USERS GREW 65% IN 2021



The number of users attacked with QakBot

– a powerful banking Trojan, in the first seven months of 2021 grew by 65% in comparison to the same period in 2020 and reached 17,316 users worldwide, demonstrating that this threat is increasingly affecting internet users. This rise has drawn the attention of Kaspersky researchers to the subject, leading them to review updates to the latest version of this Trojan.

Banking Trojans, when they have successfully infected a targeted computer, allow cybercriminals to steal money from victims' online banking accounts and e-wallets – which is why they are considered one of the most dangerous types of malware. QakBot was identified as early as 2007 as one of the many banking Trojans. However, in recent years, QakBot's developer has invested a lot into its development, turning this Trojan into one of the most powerful and dangerous among existing examples of this malware type.

"QakBot is unlikely to stop its activity anytime soon. This malware continuously receives updates and the threat actors behind it keep adding new capabilities and updating its modules in order to maximise the revenue impact, along with stealing details and information. Previously, we've seen QakBot being actively spread via the Emotet botnet. This botnet was taken down at the beginning of the year, but judging by the infection attempt statistics, which have grown in comparison to the last year, the actors behind QakBot have found a new way of propagating this malicious software," said Haim Zigel, malware analyst at Kaspersky.

DRIVING DIGITAL TRANSFORMATION WITH EFFECTIVE APPLICATION DELIVERY & SECURITY

ADRIAN TAYLOR, VICE-PRESIDENT, A10 NETWORKS, ON HOW APPLICATION DELIVERY COMPONENTS (ADC) CAN PROVIDE A UNIFIED POLICY INFRASTRUCTURE ACROSS EVERY PLATFORM, MAKING IT EASIER TO PROVIDE CONSISTENT PROTECTION FOR APPLICATIONS AND SERVICES WHEREVER THEY ARE DEPLOYED.



Adrian T aylor

The COVID-19 pandemic underscored the importance of digital resiliency in the modern era. With employees working from home, and a shift online for consumer activities from banking and retail and media, to entertainment and healthcare, ensuring application performance and application availability became a matter of survival for most companies. Whether people are working or going about their personal lives, they expect a high-quality user experience for the applications they use—every time, with no excuses—with cybersecurity they can count on to protect customer data and privacy. These demands have made the application delivery controller (ADC) one of the most important components of modern digital infrastructure.

At the same time, maintaining application performance and application availability for existing resources isn't enough to guarantee survival. In today's digital business environment, you have to stay agile and innovative to compete, grow, and thrive. In fact, even facing an

uncertain economic outlook over the past year, businesses plan to invest in digital transformation spending during the pandemic. That puts DevOps front-and-centre in digital business strategy as companies seek simple, streamlined ways to develop, deploy, change, and manage applications. The results speak for themselves: companies that use DevOps achieve 46x more software deployments and 440x faster lead time for changes. Here again, the ADC has a critical role to play in enabling the full speed and agility DevOps makes possible.

Of course, simply deploying ADCs isn't a solution in and of itself; meeting these requirements depends on having the right application delivery controller capabilities and deploying them in the right way. Here are a few things to consider, to ensure that your application delivery infrastructure is meeting the digital transformation needs of your business and customers.

Using ADCs to ensure application performance, application availability, and cybersecurity

Whether it's customers or employees who are using your applications, the experience you provide has a direct effect on digital business performance. If customers become frustrated or are unable to use your applications or services effectively, they can take their cash—and their loyalty—to a competitor. Without reliable application performance and application availability, your workforce can grind to a halt, sending waves of disruption throughout your business. Gartner estimates the average cost of downtime is \$5,600 per minute which equates to more than \$300,000 an hour.

Your application delivery controller solution can help you maintain a high-quality user experience by enabling a unified approach to managing performance, troubleshooting problems, and optimising traffic across complex environments with holistic visibility into devices, applications, policies, users, and

more across data centres and clouds. By gathering and analysing data from across your hybrid infrastructure, you can work proactively to detect anomalies sooner, diagnose problems more accurately, and resolve issues more quickly. Global server load balancing functionality can intelligently guide application traffic to the best available site for each user to ensure the best possible service.

Ensuring high availability, disaster recovery, and rapid failover across cloud providers is essential to keeping

**“SIMPLY DEPLOYING
ADC ISN'T A SOLUTION
IN AND OF ITSELF;
MEETING THESE
REQUIREMENTS
DEPENDS ON
HAVING THE RIGHT
APPLICATION
DELIVERY CONTROLLER
CAPABILITIES AND
DEPLOYING THEM IN
THE RIGHT WAY.”**

employees productive and customers satisfied. As part of its global web traffic management capability, your ADCs can assess the health and response time of each site in your environment, then make intelligent adjustments to application traffic to prevent a failed server from affecting users. Similarly, an ADC solution can help you use a public cloud as a backup for your on-premises data centre using global server load balancing to determine when and how to tap into that capacity, then reroute traffic accordingly.

While application performance and application availability are the foundation of user satisfaction and loyalty, a cybersecurity breach can destroy that trust in a flash. As ransomware attacks, DDoS, and other threats

grow in sophistication, and enterprise environments become more distributed and dynamic, cybersecurity and compliance become critical challenges. Your ADC solution can provide a unified policy infrastructure across every platform you use, making it easier to provide the same, consistent protection for applications and services wherever they are deployed. By managing authentication consistently across cloud and on-premises platforms, you can support a Zero Trust security model while providing employees with the right level of access for their needs. Protective measures such as security analytics, DDoS protection, web application firewalls (WAF), authentication, modern SSL/TLS encryption standards, and threat intelligence enable a multi-layered approach to cybersecurity for defence in-depth.

Supporting DevOps while simplifying management at digital speed

DevOps isn't just a core methodology for digital transformation—it's also a set of technical requirements. To enable development and operations teams to collaborate effectively across the software development lifecycle, you need to provide simple, streamlined ways to develop, deploy, change, and manage applications. A standard set of automation tools across platforms can help teams work efficiently, bring new staff up to speed more quickly, and ensure consistent best practices. Real-time continuous integration and delivery (CI/CD) visualisation can help teams catch costly errors before applications enter production.

The rapid pace of digital transformation can increase both cost and management complexity. By providing a single point of management across your hybrid cloud and multi-cloud environment, with comprehensive visibility and analytics for actionable intelligence, your ADC solution can help your staff use resources more efficiently, make better decisions, avoid errors, and simplify operations. 🚀

STRENGTHENING CYBER DEFENCE



Emad Haffar

EMAD HAFFAR, HEAD OF TECHNICAL EXPERTS, META, KASPERSKY, ON MODERN-DAY CYBER DEFENCE STRATEGIES.

with a fake "pending" delivery notification requesting additional payment to finalize the order. With these mailings, victims are often routed to a fake website, where they risk not only losing money but also sharing bank card details.

Several cybercriminals have also launched websites that appear to offer the opportunity to purchase parcels that could not reach the intended recipients. Of course, the parcels never arrive.

Spam messages sent on WhatsApp with requests for money were also in the bag of tricks for fraudsters during the past quarter. These scams involve several different schemes, including one that asks users to take a survey about WhatsApp and send messages to several contacts to receive prizes or other rewards.

protection layers of varied nature to every protected asset. This allows effective protection against different types of malware while making the system too well-defended for the majority of attackers.

The first layer constitutes a reliable and ultra-fast technology that detects malware by masks and hashes. The second layer uses emulation, which runs suspicious code in an isolated environment. Both binaries and scripts are emulated, which is critical for protection against web threats.

The third layer is a classic detection routine. It's a tool that allows Kaspersky experts to write a code and deliver it directly to the user in databases. This technology is truly irreplaceable; it complements the solution with decryptors for ransomware and unpackers for legitimate packers. The fourth layer assumes the use of machine learning models on the client's end. The models' high generalisation ability helps to prevent the loss of quality in detecting unknown threats, even if an update of databases was not available for more than two months.

The fifth layer is cloud detection using big data. It leverages threat analytics from all endpoints in Kaspersky Security Network, which, in turn, enables an unprecedented reaction to new threats and minimising false positives.

The sixth layer is heuristics-based on

2 021 has been an interesting year for spam and phishing attacks. What are some of the main attack trends being seen this year?

With the significant increase in online shopping today, criminals have been exploiting these transactions by targeting the final step of the purchase, the delivery. The attack scams witnessed recently are related to the shipments via courier delivery services, where fraudsters call, mail or send SMS messages to the victims

How can CIOs and other company bosses build an effective defence mechanism against hackers?

Genuine full-proofed cybersecurity should be based on a multi-layered approach that blends various protection techniques, from classic AV records to behaviour-based detection with deep learning models. Because newer, more sophisticated cyberattacks try to overcome existing protection, it is crucial to mount layered defences, covering both different levels of infrastructure and applying multiple

execution logs. There is no more fail-safe way to catch a criminal than catching him in the act. Instant backup of data impacted by a suspicious process and automated roll-back neutralise malware the moment it's detected.

The seventh layer involves gathering real-time behavioural insights on files to create deep learning models. The model is capable of detecting a file's malicious nature while analysing a minimal amount of instructions. This helps to minimise threat persistence, and machine learning provides high detection rates even when a model update is unavailable for a long time.

Using machine learning on various layers of a file antivirus subsystem is, in its very essence, proof of Kaspersky's functional, next-generation approach to protection.

What do you think are the main challenges companies face while implementing a cybersecurity framework?

We believe that organisations must allocate a specific budget to cybersecurity. This is, of course, challenging as C-suite executives want to see a direct return on any money spent.

Research shows, however, that even smaller organisations are also under attack. According to Kaspersky, 36% of micro-enterprises and 48% of SMBs experienced data breaches in 2019, up from 30% and 46% respectively the year before.

The average cost of a security compromise for a small to medium business (SMB) stood at US \$108,000. Approximately half of this amount stems from damage to information and infrastructure, the rest resulting from disruption to normal operations. It's therefore vital to make the case that this an investment in cybersecurity is an investment in business continuity and, thus, the company's future.

Cyber resilience is a term not too many people are aware of. How vital is a

robust cyber resilience strategy for organisations & what are some of the key things to keep in mind while doing so?

As mentioned, an effective cybersecurity strategy incorporates multiple layers of security techniques, and technologies. Given the changing nature of the threat and the scarcity of skillsets in this area, we believe the key things to keep in mind when building a robust cyber resilience strategy for organisations is to implement a security solution like Kaspersky's Managed Detection and Response (MDR) service. MDR providers can take care of a range of essential cybersecurity tasks, including the installation and maintenance of anti-virus software, firewalls and applications; virtual private network (VPN) management; e-mail monitoring and intrusion detection. A managed service provider may work remotely or enable internal staff to react on their own following instructions from the MDR. The latter is helpful at the beginning of a partnership, as a customer needs to

“BECAUSE NEWER, MORE SOPHISTICATED CYBERATTACKS TRY TO OVERCOME EXISTING PROTECTION, IT IS CRUCIAL TO MOUNT LAYERED DEFENCES COVERING BOTH DIFFERENT LEVELS OF INFRASTRUCTURE & APPLYING MULTIPLE PROTECTION LAYERS OF VARIED NATURE TO EVERY PROTECTED ASSET.”

ensure that the recommendations work with their network and processes. Also, some prefer to respond on their own in case critical assets, such as computers belonging to executives, are involved.

Individual behaviour is often overlooked while putting together a cyber-defence strategy. How important is individual behaviour in cybersecurity & how can such behaviour be made more accountable?

It is well known that humans are the weakest link in the cybersecurity chain. There are well established best practices that everyone should follow, including keeping passwords secret, beginning wary of opening unsolicited e-mails and exercising caution opening attachments, and using only work accounts and approved apps to handle company data. Raising cybersecurity awareness and ongoing end-user training is essential. Kaspersky offers a unique solution among security awareness training courses, combining content based on Kaspersky's 20+ years' experience in cybersecurity and advanced learning and development methodology developed by Area9 Lyceum on Rhapsode, the world's first four-dimensional adaptive learning platform.

Finally, there is a lack of skills in cyber threat mitigation, even at the top levels. How do you think this can be addressed?

We believe there is a need for training at all levels of organisations, but different levels need different levels of training. With the Kaspersky Automated Security Awareness Platform (ASAP), organisations can simplify through automation. It takes just 10 minutes to simply upload a user list, divide users into groups and set target levels for each group. The platform builds an education schedule for each group, based on pace and target level, as well as delivering actionable reporting and recommendations. 📌

WHY YOU SHOULDN'T POST YOUR VACCINATION CARD ON SOCIAL MEDIA

DUANE NICOL, CYBERSECURITY EXPERT AT MIMICAST, TELLS SECURITY ADVISOR WHY EVEN SIMPLE LIKES AND COMMENTS ON SOCIAL MEDIA CAN PROVIDE CRIMINALS WITH IMPORTANT INFORMATION THAT MAKES THE VICTIMS— AND EVENTUALLY THEIR EMPLOYERS— VULNERABLE.



Duane Nicol

“People are rightly excited about getting their COVID-19 vaccinations, and many happily post their vaccine record

cards to their social media profiles to share the good news with friends and family. However, friends and family may not be the only ones watching. Cybercriminals could use the information – such as names and dates of birth – to develop believable social engineering attacks.”

Social engineering attacks can take several weeks or even months as criminals need time to get to know their victims. But Nicol explains that the more information you share the easier you make it for a criminal.

How would such an attack work in simple terms? “Let’s say Mr Cybercriminal wants to target a bank. He goes to LinkedIn to see who works there, finds a few candidates, and goes onto their Facebook and Twitter accounts to get more information. One of the candidates, let’s call him Bob, recently posted a photo of his vaccine record with his name, date of birth, first vaccination date, manufacturer and date of the second scheduled vaccination,” explains Nicol.

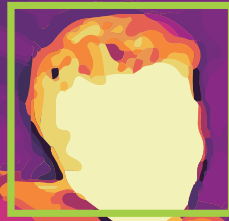
From here, Mr Cybercriminal sends an email to Bob’s work address asking him to confirm his second vaccination date. The email appears to be coming from a trusted source such as the health authority or service responsible for vaccine administration in his region. The link in the email seems legitimate, the branding is on point and the information about his vaccination record is all accurate, so Bob goes through the steps to set up an account. Bob, who easily forgets passwords, uses the same password he uses to log in to his company network. What he doesn’t realise is that he’s entering his personal information into a fraudulent website. Now Mr Cybercriminal can use Bob’s credentials to access the network of the bank he’s targeting.

Of course, most organisations will have layers of protection, such as security questions. For example, when logging in from a new device they might ask ‘what is your mother’s middle name?’ But criminals are always one step ahead. A seemingly harmless post about how your cartoon character name is your mother’s middle name plus the last thing you ate, could be answering a security question for a criminal stalking your social channels.

“Once in, the cybercriminal can do untold damage to the bank’s network, access confidential files, impersonate key stakeholders within the organisation, commit fraud on a massive scale and even infect the network with malware that could take services offline and lead to catastrophic financial losses and severe damage to the bank’s reputation.”

Nicol says the accessibility of personal information on social media arms cybercriminals with vital tools that they can use in the service of fraud and other crimes. “Even simple likes and comments can provide criminals with important information that makes the victim – and ultimately their employer – vulnerable. End users in the region need to take heed and maintain safe social media habits to limit the opportunities for cybercriminals.” 🔒

36.5° C



Hikvision Temperature Screening Thermal Solutions

SAFER, FASTER, SMARTER



Contact-free



Multi-person detection



1s measurement



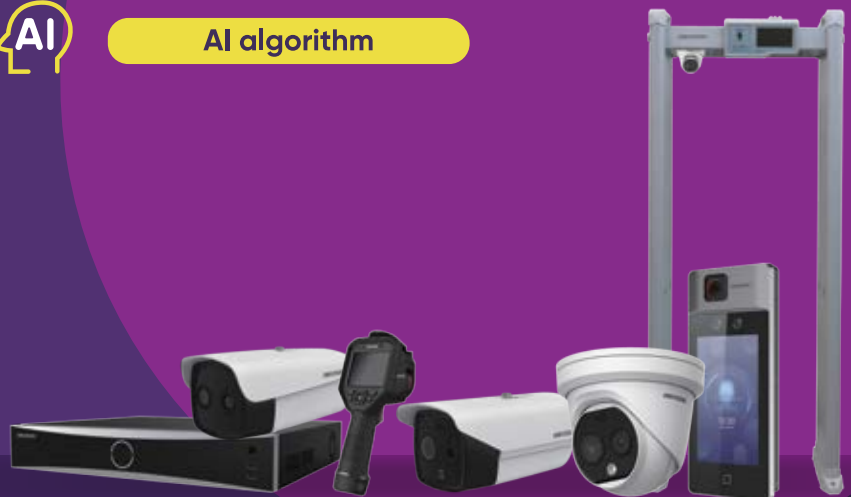
AI algorithm

Thermographic
Cameras

MinMoe Terminals

Metal Detector Door

DeepinMind NVRs



Temperature Screening
Thermal Cameras

For more information, please scan the QR-Code to visit
our Temperature Screening Thermal Solution page.

HIKVISION

www.hikvision.com

DO YOU KNOW YOUR BREACH LIKELIHOOD?

CHERIF SLEIMAN, CHIEF REVENUE OFFICER
AT SAFE SECURITY, TELLS ANITA JOSEPH WHY
KNOWING IS CRITICAL TO BUILD A SAFER DIGITAL
FUTURE. A SECURITY ADVISOR EXCLUSIVE.



Cherif Sleiman is a man on a mission - a mission to make the world a safe place as its journey into cyberspace gains momentum. In fact, his recent

career move to the

Palo Alto based startup SAFE Security is testament to this commitment. SAFE Security, unlike any other cybersecurity organisation today, takes a "proactive"

approach to cyber defence as opposed to the "reactive" approach commonly being practiced. Its focus on cyber risk quantification is a unique first step in an attempt to recognise and classify cyber risks and the steps that can be taken to mitigate their impact.

Says Sleiman about the move: "My decision to join SAFE Security was not a light one. I'm very, very selective and opinionated about what I want to do. So when I crossed paths with SAFE Security, I felt that this is my home for the next few years. The company is a pioneer in

the field of cyber risk quantification and breach prediction - a new and upcoming field that is critical to creating a safer digital future. SAFE Security is one of those amazing organisations that has seen much acceptance by stellar people and organisations out there including John Chambers, British Telecom, Paypal and many others who realised the opportunity and potential that SAFE Security has in shaping the future of the tech industry and making it safer."

So, what is cyber risk quantification and why is it so important today?

SAFE Security, a startup company headquartered in Palo Alto, California, backed by British Telecom & John Chambers, has announced its foray into the Europe, Middle East & Africa (EMEA) region.

SAFE Security helps organisations measure and mitigate enterprise-wide cyber risk using its Security Assessment Framework for Enterprises (SAFE) platform.

The company enables CISOs, CIOs and other risk and compliance officers to visualise, understand, and quantify their cyber risk. SAFE Security streamlines boardroom discussions and decisions focused on cyber risk exposure quantification, prioritisation of key cyber risk initiatives, security budget allocation and cyber insurance.

SAFE Security will join hands with management consultancy organisations, GSIs, MSPs, security specialist VARs and security alliance vendor partners to institutionalise the practice of Cyber Risk Quantification and Breach Prediction within organisations that are deemed critical national infrastructure across EMEA.

According to Sleiman: "Cyber risk quantification involves measuring and mitigating enterprise-wide cyber risk in real-time by aggregating signals across five different vectors of assessment - people, process, technology, cyber security, and third-party partnerships - to dynamically predict the breach likelihood and assign a dollar value to the risk an organisation is facing. Cyber risk quantification is not just important, it is extremely vital and foundational to how organisations need to run and manage their digital footprint, moving forward. It's no longer an option."

To substantiate this, he comes out with a few "bold" statements that showcase the pitfalls of the practice of cybersecurity as it exists today.

Firstly, "It doesn't matter how much effort, energy, focus and money we spend to secure ourselves, all of it just seems futile. We listen to analysts, read the journals, buy the products and the antidotes that the experts tell us we need to better secure our people and organisations. We follow frameworks like SASE and Zero-Trust and we pivot security from the datacentre to the edge. We feel like we're doing everything we're being told. And yet, we never once, even for a minute, feel safer."

The second statement which is thought provoking: "If you're piling up all these products and listening to all the experts, and still falling short of the noble objective of making things safer, the question is: Why?"

He has the answers as well: "Because there is a severe lack of proper contextual visibility and for the most part, organisations are still product focused when approaching the security of the enterprise. To put it simply: When you know the risks involved, you're able to take informed decisions about safety and security. Safety inspires confidence, confidence inspires courage, courage

inspires action. So, safety is all about knowledge. The problem we have today is that organisations are throwing so much money, resources and products at a problem, but the mindset still hasn't changed. The fallacy is in thinking that the organisation continues to be centred around a data centre where there's only one way in and one way out. We are putting all our bodyguards there thinking that we have done a good job when in fact today's organisation is borderless and entry points are numerous."

According to him, the Covid-19 pandemic should serve as an eye-opener.

"Ever since the start of the pandemic early last year, there's been an average of 5-7 years' worth of digital acceleration, both in the back-end and the front-end of the enterprise, in under twelve months. No organisation in the world could have planned for Covid or had a business continuity plan that factored in an event like this. But with remote working and the hybrid workplace becoming the norm, organisations had to embrace Cloud Computing and SaaS as a matter of survival, even though they might have been resistant to these technologies to begin with."

"Transitioning to cloud-based technologies has created the 'Swiss Cheese' architecture, as I'd like to put it, with many holes, and with so many ways in and out of the organisation," he says. "Your employees are all over the place, connecting to workloads and data that's now in a multi-cloud fabric dispersed all over the place, using different devices from different locations. In addition, your customers and suppliers have also changed the way they do business with you. They're all over the place as well. How can you really expect to secure every aspect of every interaction? So, the number one issue we have today is that we have no visibility, as the digital

$$\text{Decision} = \frac{\text{Revenue / productivity benefit / Cost Reduction}}{(\text{Cost}) \text{ (Risk)}}$$

Only a good decision if the result is greater than 1, and the higher the, better the decision

For example:

25% Cost Savings

.67

=

1

(.75) (2)

Bad decision

Doubling Revenue

1

=

2

(1) (2)

Bad decision

footprint is so vast. We do not have the right knowledge of our cyber risk and therefore everything we do is based on hope and best intentions. But the fact of the matter is that we are stuck in a vicious cycle of more breaches every time we make more technology investments."

The second problem, in his opinion, is that for the longest time, the concept of risk has been focused around policies and procedures in a brick and mortar manner. "When we started becoming more digitally inclined, we realised that cyber risk assessment should not just consider the basic organisational architecture, but other moving parts including people, technology and

partnerships that are scattered everywhere. Take business partnerships as an example - all organisations have suppliers, partners, etc. We realised that if a company does a great job at securing its infrastructure and its people, that's not enough. No company is an island and if it is to thrive in today's world, it has to deal with customers, suppliers and partners where a lot of information has to be exchanged. And if a partner that an organisation is interacting with does not adhere to any kind of data privacy policy, then data can leak through their network, despite an organisation's best efforts. So, assessing your partners' risk profile and practices

and how they secure their data and your own data is important before you ink a contract with them, however attractive the terms of the contract may be."

"Assessing your cyber risk is also about assessing your technology infrastructure and cyber security products and capabilities to score every aspect of your organisation - every end-point, server, workload, application, system, database, storage, middleware, etc regardless of whether it is on premise or in the cloud. There should be an integrated and objective view on a single dashboard that aggregates data from all these products along with prioritised actionable insights on what's failing and what is working. Secondly, the impact of these vulnerabilities has to be represented in a universally understood language - business consequences, that could be the financial impact, loss of reputation, customer retention, etc depending on business priorities. This is something that doesn't exist today. And when you do that quantification, with all the insights, you are able to make decisions. What are the risks

"THE PROBLEM WE HAVE TODAY IS THAT ORGANISATIONS ARE THROWING SO MUCH MONEY, RESOURCES AND PRODUCTS AT A PROBLEM, BUT THE MINDSET STILL HASN'T CHANGED."

I need to mitigate? What are the minimal risks that I can accept? And what are the risks I can transfer to cyber insurance?"

Security & risk management leaders including CFOs, CIOs, CISOs have more than enough cybersecurity tools and services. In fact, the average organisation has more than 40 cyber security products to manage, but what is missing is a real-time objective view into the effectiveness of their cybersecurity program, investments, and tools, and this is where SAFE is disrupting the market.

SAFE Security brings rich insights to CXOs about their cyber risk posture with the real-time, enterprise-wide breach-likelihood score.

"With SAFE Security, we have a common language that binds very different roles and functions from the board down to the security operations team," Sleiman adds.

That brings us to the next important question: How aware are organisations of the need to quantify risk?

He says: "There's no doubt that our region has in the past, and continues to experience, plenty of geopolitical conflicts. This creates insecurity among organisations in certain sectors and with it a pressing need to protect the infrastructure. On a positive note, there's an incredible amount of regional awareness about cybersecurity. However, I don't think enterprises are going about it with the right mindset. IT leaders need to understand that they can greatly enhance their security posture with the same effort, money and resources spent, if only they do things differently and in a more strategic manner. That is really what SAFE Security will focus on for the next few months as we roll out awareness sessions and campaigns with partners. Our mission as a company is anchored on making the world a safe place and we'll spare no effort in this regard."

"THE AVERAGE ORGANISATION HAS MORE THAN 40 CYBER SECURITY PRODUCTS TO MANAGE, BUT WHAT IS MISSING IS A REAL-TIME OBJECTIVE VIEW INTO THE EFFECTIVENESS OF THEIR CYBERSECURITY PROGRAM, INVESTMENTS, AND TOOLS, AND THIS IS WHERE SAFE IS DISRUPTING THE MARKET."

With these goals in mind, SAFE Security is making sure it is leaving no stone unturned to become the de facto standard for measuring and mitigating risk in the cyber world. "What appeals to me about SAFE Security is the company's approach to engaging with business leaders in a way that bridges the divide between technology and business. Risk is the ownership of C-level management. So, we've been extremely selective in who we partner with, because we want to form alliances with organisations that are able to have the inroads to meet with appropriate organisational stakeholders, in order to help them quickly."

When it comes to how SAFE will make all of this happen, Sleiman says that they will partner with like-minded organisations that are focused on protecting the region's mission critical infrastructure. He said that the company's strategy is centred around five routes to market: 1) The consultants that are writing the digital blueprint for organisations – companies like Accenture, Deloitte, KPMG and the like. 2) The global SIs – the ones implementing these digital blueprints – Infosys, Wipro, Tata, Capgemini and so on, with their multinational footprints. 3) The Managed Service Providers – the ones who take the products and make

it part of their network so it becomes a utility and a service that can be delivered to organisations that don't want to do it themselves. 4) The VARs – that have built a cybersecurity practice and understand risk in the cyber world and 5) Alliances – Elite cyber security vendors that sell a lot of diverse products. By partnering with SAFE, they can assess how well their solutions are implemented and can plug any gaps that are uncovered.

So, how future-proof are SAFE Security's products?

Sleiman points out that SAFE Security is not a defence mechanism or an in-line technology. "We integrate and ingest signals and data from over 100 Cyber Security vendors and use concepts like Bayesian Network and Monte Carlo Simulations that are used by Financial and Insurance companies to assess risk. We also leverage a comprehensive set of standards and frameworks such as NICE, NIST, ISO, CIS, STIG, MITRE, and many others. We have codified all the controls in these standards and have done an incredible amount of automation in the way we apply all these controls to people and various assets in the organisation to have a prescriptive and quantitative score indicating breach likelihood and dollar value impact. All of it bubbles up into the overall organisational risk... This is

CISO Priorities



- Modernize enterprise security architecture
- Create a culture of cybersecurity
- Keeping up with emerging, evolving privacy laws
- Building continuity plans to account for global events

something really unique in the industry.”

Sleiman also notes that at the end of the day, none of it is as complicated as it sounds.

“There’s an incredible amount of intimidation for any professional, no matter how skilled, when they hear about things like AI, Machine Learning, Automation & Predictive Analysis. There’s also no doubt that there is a huge amount of complexity and genius behind these technologies. However, the great thing is that organisations don’t have to deal

with these complexities - we’re bringing it to you as a utility in a natural language that is easy to use. Of course, you need to understand the basics like your network etc, in order to optimally configure the solution. But you’re not going to have to tweak and tune AI or any of those complicated technologies under the hood. It’s like flipping on a light switch - you press the switch and the light comes on. You’re not involved with the wires or the circuit breakers or any of the

intricacies. What we do is similar. We’ve packaged all these intricate technologies into a SaaS-based product, and like the underlying principles of SaaS, it is all about simplification,” he adds.

Sleiman reiterates that the mistake businesses and governments make is they think they can use new technologies without making changes to their underlying business processes and regulatory frameworks. The rise in digital has created more security risks. And these risks don’t only extend to government agencies or financial service firms. It is integrated into our supply chain, which impacts every company and every person.

In conclusion, Cherif indicates that if we are to break the current vicious cycle of ‘the more we invest, the more we get breached’, then a real bold step is required by various government bodies and ministries as well as enterprise security and risk management leaders to embrace a Cyber Risk Quantification mindset and institutionalise such practice in their organisations. Only then, we can say we are heading to a safer digital future. 🙌

"ASSESSING YOUR CYBER RISK IS ALSO ABOUT ASSESSING YOUR TECHNOLOGY INFRASTRUCTURE AND CYBER SECURITY PRODUCTS AND CAPABILITIES TO SCORE EVERY ASPECT OF YOUR ORGANISATION - EVERY END-POINT, SERVER, WORKLOAD, APPLICATION, SYSTEM, DATABASE, STORAGE, MIDDLEWARE, ETC REGARDLESS OF WHETHER IT IS ON PREMISE OR IN THE CLOUD."

EXCLUSIVE NETWORKS BEGINS PROCESS OF GOING PUBLIC



Jesper Trolle

JESPER TROLLE, CHIEF EXECUTIVE OFFICER AT EXCLUSIVE NETWORKS, SAYS THE IPO WILL SUPPORT THE COMPANY'S MISSION TO HELP DRIVE THE TRANSITION TO A TOTALLY TRUSTED DIGITAL WORLD.

Exclusive Networks S.A. has announced the filing of its registration document with the AMF under the number I. 21-044, the first step in Exclusive Networks' contemplated initial public offering on the regulated market of Euronext Paris, subject to market conditions and the approval by the AMF of the prospectus for the offering. The registration document contains a detailed description of the Company, in particular its business, strategy, financial condition and results of operations, as well as related risk factors. Exclusive Networks draws the public's attention to the risk factors contained in Chapter 3 of the registration document.

Commenting on the announcement, Jesper Trolle, Chief Executive Officer at Exclusive Networks, said: "Exclusive Networks is a global cybersecurity specialist, with a strong track record of profitable growth. Our proposed IPO on Euronext is a natural next step for us, and recognises three vital pillars of our success – our people, partners, and growth strategy. First, without the know-how and talent of our people, our growth would simply not be possible. Second, we have built our success on strong, enduring relationships within the complex cyber ecosystem, with vendors and channel partners. Exclusive Networks is the partner of choice for more than 240 leading vendors. Exclusive Networks supports the growth and expansion plans of vendors, offering local support to enable them to reach more than 18,000 resellers around the world. Third, we have a clear strategy in place to continue to deliver growth, and an IPO will support our mission to help drive the transition to a totally trusted digital world.

In the last 18 years we have made

the journey from a small private company to a global cybersecurity specialist, with a 36% gross sales CAGR since 2013. Cybersecurity is a highly attractive market, estimated to be worth €58bn in 2020 and growing at a 9% CAGR from 2020 to 2026. The cyber ecosystem is getting more and more complex, the channel selling cyber products is fragmented, and technology is evolving very quickly to combat the growing sophistication in threats and cyberattacks. This creates demand for a cyber specialist like Exclusive Networks in the long-term, and we look forward to bringing even greater value to our vendors and partners, by executing on our mission to drive the transition to a totally trusted digital future."

About Exclusive Networks

Exclusive Networks is a leading global specialist in innovative cybersecurity technologies, providing services to accelerate the sale of cybersecurity disruptive and digital infrastructure technologies on a global scale. Exclusive Networks helps cybersecurity vendors scale their businesses globally, and offering channel partners (such as value-added resellers, system

integrators, telcos and managed service providers) expertise, disruptive technologies and services to fit the needs of their corporate customers. Exclusive Networks also works with several vendors offering solutions in specific sub-segments beyond cyber.

Exclusive Networks excels by combining global scale with local execution. With offices in 40 countries and the ability to service customers across five continents and in over 150 countries, Exclusive Networks, headquartered in France, offers a "global scale, local sale" model. This model enhances performance in local operations by providing both global and local support. This approach has enabled Exclusive Networks to (i) develop one of the world's broadest portfolios of cybersecurity solutions from over 240 leading vendors and (ii) develop a worldwide customer base, consisting of over 18,000 VARs, SIs, Telcos and MSPs, indirectly serving more than 110,000 end-customers. Over the period from 2018 to 2020, Exclusive Networks engaged in business in more than 124 countries.

Exclusive Networks' approach enables vendors to adopt a simple and agile go-to-market model in relation to their cybersecurity and digital infrastructure solutions, while benefitting from Exclusive Networks' local expertise and market knowledge in each jurisdiction where it operates. Exclusive Networks' scale is equally important to its customers as their own end-users may be located in multiple regions of the world. In addition, Exclusive Networks helps its customers through its expertise in vendor selection as cybersecurity and digital infrastructure solutions become ever more complicated and keep evolving in the face of increasing cybersecurity threats. 📌

"IN THE LAST 18 YEARS, WE HAVE MADE THE JOURNEY FROM A SMALL PRIVATE COMPANY TO A GLOBAL CYBERSECURITY SPECIALIST, WITH A 36% GROSS SALES CAGR SINCE 2013."

GOVERNMENT AGENCIES CAN PREVENT CYBERATTACKS THROUGH GOOD CYBERSECURITY HYGIENE & EMPLOYEE EDUCATION



Wissam Saadeddine

WISSAM SAADEDDINE, SENIOR MANAGER – MENA AT INFOBLOX, TELLS SECURITY ADVISOR HOW WITH THE VAST MAJORITY OF OFFICE-BASED GOVERNMENT EMPLOYEES WORKING AT HOME, AGENCIES NEED TO FOCUS ON THE BASICS OF IDENTITY MANAGEMENT; IMPLEMENTING ZERO TRUST IN ORDER TO PROTECT NETWORKS FROM UNTRUSTED USERS AND ENSURING THAT DATA IS PROTECTED FROM UNAUTHORISED EGRESS AND ACCESS.

While working in the public sector and private sector have many differences, one characteristic is similar: cybersecurity and threats. Both sectors feel the pain of not having a sufficient community of trained and available security staff to hire, both are constant targets of phishing and related social engineering attacks and both are trying to balance the three-pronged attacks of the pandemic, the relocation of employees to work-from-home status and increased risks from attacks on cloud assets.

The current pandemic is having a major impact on all levels of government. Aside from the financial impact the pandemic is having on the private sector, government IT professionals are also facing the following challenges:

- Workers are being required to work from home
- IT and security staffs must provide WFH employees with new equipment, which has major implications for IT budgets
- Users are connecting to government networks from untrusted and often compromised home networks
- Users are employing personal equipment and IoT devices to connect to government networks and clouds that might not be secured to the governmental agency's security standards

However, governments have other concerns as well. Government operations can potentially impact much larger groups of people than a corporate attack. Depending on the government entity targeted, the effect could impact critical infrastructure at all levels. The COVID-19 effect of draining

critical financial resources to fund purchases of hardware and software for newly displaced employees, plus expenses for significant increases of cloud services and, in some cases, a forced digital transformation from on-premises data center to cloud-based assets, is putting a strain on both financial and staffing resources.

From the citizenry perspective, the pandemic has opened the proverbial Pandora's box of fake "official" websites devoted to COVID-19, misinformation from websites purporting to be the Centers for Disease Control and Prevention and other government and medical facilities that actually are watering holes for malware and ransomware attacks on hospitals delivered in emails purporting to be information about COVID-19.

A joint advisory group from U.S. and U.K. security agencies also was formed to protect the intelligence communities from becoming victims of attacks, particularly from advanced persistent threats from groups targeting individuals and organisations with malware. In March 2020, Infoblox observed a malicious spam (malspam) email campaign that used a fraudulent Coronavirus alert from the World Health Organization (WHO) to deliver Trickbot banking malware. We also observed a series of campaigns using COVID-19 or Coronavirus-themed spam emails to distribute the Agent Tesla information stealer (infostealer).

What can government agencies do to defend themselves against such attacks?

While public and private sectors have some differences when it comes to issues such as disclosure and confidentiality, the basis is the same. At the core is user education. Helping government employees understand good cybersecurity hygiene is essential. With the vast majority of office-based government employees working at home, agencies need to focus on the basics of identity management; implementing zero trust in order to protect networks from untrusted users, devices, applications and network connections; and ensuring that data is protected from unauthorised egress and access.

For those governmental agencies without existing threat intelligence capabilities, now would be a good time to invest in a comprehensive program that includes a mix of traditional data feeds, specialized feeds focusing on specific requirements for a given agency, an open source intelligence (OSINT) feed and greater emphasis on understanding the threat intel an agency already is generating from its existing SIEM systems and related log systems.

Government agencies also should take advantage of several emerging technologies to further enhance their existing security policies. For example, security orchestration, automation and

FROM THE CITIZENRY PERSPECTIVE, THE PANDEMIC HAS OPENED THE PROVERBIAL PANDORA'S BOX OF FAKE "OFFICIAL" WEBSITES DEVOTED TO COVID-19."

response (SOAR) enhances the speed and reliability of existing operations. For cloud-based operations, a cloud access security broker (CASB) is on-premises or cloud-based security policy enforcement placed between cloud server consumers and providers. It interjects enterprise security policies as cloud-based assets are accessed.

Continuous management and monitoring add another dimension to protecting government networks. As a key target of bad actors and nation-state cyberattackers, continuous monitoring is essential; any lapse can let attackers have access to a system, even if just momentarily.

So, how can government agencies protect themselves and their employees from potential losses? Generally, the best practices for corporations apply to government agencies as well.

Cybersecurity guidelines for government organisations

- Use advanced DNS protection to defend against the widest range of DNS-based attacks
- Use a DNS firewall that automates malware protection.
- Detect and prevent data exfiltration by utilizing DNS-based analytics.
- Use a centralised, cloud-managed, provisioning, management and control solution, designed with the modern borderless enterprise in mind. This is what is needed to eliminate the management complexity and bottlenecks of the traditional branch office DDI (DDI is the integration of domain name system, dynamic host configuration protocol and IP address management into a unified service or solution).
- Deploy a virtual DDI appliance on a public or private cloud, which can enable you to deploy robust, manageable and cost-effective appliances.
- Have an Incident Response and Backup Plan. Test the plan on a consistent basis and adjust as necessary.
- Have a consistent security policy across all platforms. For example, if you are leveraging cloud services, ensure they are secured as you would on premises.
- Ensure you are actively monitoring and managing DNS within your organization.
- Use comprehensive threat intelligence to proactively block malicious DNS threats.
- Monitor and manage the behavior of DNS in your environment — black-lists are not enough, you need to ensure that the protocol is behaving as appropriate.
- Restrict use of DNS over TLS (DoT) and DNS over HTTPS (DoH) on assets and on the network.
- Know where your users (assets) are going from a DNS perspective, no matter where they are located (on premises, working remotely, etc.). Have a 360 degree view of all assets.
- Automate responses where possible to leverage your current infrastructure. There is no silver bullet when it comes to security, but you can solidify your posture by using defense in depth and automation. 🛡️

VERITAS EXECUTIVE HIGHLIGHTS BENEFITS OF SAAS ADOPTION



Arthur Dell

SECURITY MIDDLE EAST SPOKE TO ARTHUR DELL, TECHNOLOGY LEADER AT VERITAS TO FIND OUT MORE ABOUT THE BARRIERS FACING ENTERPRISES OVER CLOUD DATA PROTECTION, WHY SAAS HAS EMERGED AS THE PREFERRED MODEL OF ADOPTION – AND HOW ITS RECENT ACQUISITION OF HUBSTOR WILL ENHANCE ITS SECURITY OFFERING TO ITS CUSTOMERS.

What are some of the biggest barriers to cloud data protection faced by enterprises today?

One big barrier is the widespread but mistaken belief that the cloud service providers are responsible for backing up the data. In fact, customers are responsible for protecting their own SaaS data, but they often don't realise this.

Performance and scalability can be a challenge, given the volume of data that modern businesses generate. Especially when initially setting up a backup, companies can have many PBs of data to capture, and some systems are unable to accomplish this within an acceptable timeframe.

Data sovereignty is a challenge for many organisations, as different countries have different laws about how and where data can be stored, which ultimately requires multiple distributed global data stores.

Why is enterprise adoption of SaaS becoming so popular?

If you were to pose this question to the decision-makers at different organisations, you'd likely receive different answers, but at the core, their reasons for choosing SaaS over on-premises comes down to the following:

Lower cost—SaaS costs for the organisation will be less than the total of individual applications for each user.

Ease of deployment—There's no actual software deployment needed. All users need is a web browser or a client they can download and install.

Simpler purchasing process—Rather than having to count users to ensure the purchase of enough license keys, SaaS has a far simpler subscription pricing model.

Simple support for remote users—From the SaaS platform's point of view, all users are remote, including those working on-premises, allowing all of them

to receive the same support regardless of their location.

Reduced management effort—On-premises or per-desktop software requires administrators spend time and effort monitoring and managing the software and its infrastructure. Management tasks associated with SaaS applications are minimal, and the SaaS provider manages the infrastructure.

Tell us more about Veritas's Enterprise Data Services platform-what is its USP?
NetBackup SaaS Protection is the optimal data protection solution for data in your SaaS applications.

It protects your SaaS data against both accidental or malicious deletion, as well as protecting it from ransomware or other forms of data corruption.

NetBackup SaaS Protection was designed from the ground up to be an enterprise SaaS application allowing you to protect your data on the most commonly-used SaaS applications.

NetBackup SaaS Protection provides the performance, scalability, and hardened security that enterprises need and is unique in offering all its benefits through a dedicated single-tenant instance and for its ability to automate data sovereignty compliance.

What prompted the decision to acquire HubStor? Can you give us a background to the acquisition?

Veritas recognised the need for SaaS backup, and the increasing vulnerability due to the widespread misconception that it was being handled by the cloud service providers. The company was looking for the best way to address this market and to extend its leadership in enterprise data protection.

Veritas spent over six months understanding HubStor's capabilities. We were impressed with the traction that they had achieved in a very short period.

HubStor offered a granular, scalable, easily configurable solution for SaaS

VERITAS PROVIDES A HIGHLY SCALABLE, UNIFIED PLATFORM TO PROVIDE RELIABLE PROTECTION AND ROBUST RESILIENCY ACROSS THE ENTIRE INFRASTRUCTURE."

Backup that had already established an impressive track record in the enterprise space, and even within the Veritas customer base.

Veritas has over twenty years of successful partnership with Microsoft, so the fact that the HubStor solution is tightly integrated and fully optimised for Azure was attractive.

How will the addition of HubStor to the Veritas portfolio enhance cloud data protection & security for customers?

Bringing HubStor into the NetBackup portfolio extends that platform into key SaaS applications. With HubStor, now re-branded as NetBackup SaaS Protection (NSP), we support Microsoft 365, Box and Slack, and the plan within the next six months to a year is to further expand the Salesforce presence beyond Slack.

This supports our strategy of the Enterprise Data Services platform protecting data wherever it may be and however the customer wishes to do it, by protecting those key SaaS applications.

A standardised, consistent architecture across the data estate is critical to reduce risk, yet most solutions fail to provide comprehensive support. How will the addition of HubStor to Veritas address this issue?

Veritas provides a highly scalable, unified platform to provide reliable protection and robust resiliency across the entire infrastructure, which is vitally important

for enterprise customers.

Modern enterprises must manage heterogeneous environments, with data stored locally and remotely with both physical and virtual servers, public and private clouds, and an ever-increasing volume of mission critical data.

Veritas' unified suite of products is designed to handle this complexity and scale, and the addition of NetBackup SaaS Protection strengthens our offering for SaaS Data, as increasing numbers of enterprises embrace the SaaS model.

Threats such as ransomware and accidental/malicious deletion are widespread today. Does the Veritas NetBackup SaaS Protection solution take this into account?

Yes, NetBackup SaaS Protection provides a completely separate backup of a customers' SaaS data that is secure and scalable, and under their control. In the event that the data stored within the SaaS environment is lost through accidental or malicious deletion or is damaged by ransomware, the customer can revert to a recent backup copy of the data - and can avoid significant interruption or data loss. Furthermore, NetBackup SaaS Protection works with immutable storage to prevent attackers from similarly damaging the backup data.

Why is Automatic Compliance Enforcement important? How does the new NetBackup solution ensure this?

Regulatory compliance is absolute by definition. A single file that is inappropriately deleted or stored in the wrong location is enough to render the entire solution non-compliant. Reliance on manual processes is therefore dangerous.

NetBackup SaaS Protection features fully automated compliance enforcement that allows customers to set up their policies and then rely on the system to automatically capture information and store it in compliance with legal and regulatory requirements. 🔑



tahawultech.com

CISO50 AWARDS 2021

The CISO 50 & Future Security Awards 2021 organised by CPI, celebrated and recognised accomplishments in the regional IT security landscape. The awards, which took place at the Habtoor Grand Hotel in Dubai in September, celebrated and recognised CISOs & industry visionaries who display uncompromising dedication and commitment towards creating a cyber secure world, even in the midst of challenging market conditions. In particular, it celebrated the role of the CISO/CIO and other security decision makers as they lead the way in bolstering cybersecurity, thinking outside the box, stepping up and helping businesses navigate the challenges brought on by the new normal. We bring you the full list of winners across all categories.



Aliasgar Bohari
Zulekha Hospital



Hani Bani Amer
ENOC



Harsh Daftary
Emirates NBD Bank PJSC



Nico Putter
Lamprell Energy



Binoy Balakrishnan
AW Rostamani Group



Shah E Room Khan
Emirates College of Technology



Mohammad Hennawi
NAFFCO



Nithin Geo Thomas
Amity Education Middle East



Eric Gayet
Majid Al Futtaim Properties



Mustansir Aziz
Gulf Diagnostic Center Hospital



Mohamed Sabah Al Khalaf
Dubai Holding LLC



Manan Shah
Avalance Global Solutions



Shijin Prasad R.S.
Cure Medical Centers



Rajesh Sivarajan
Geodis Freight Forwarding LLC



Irshad Mohammed
VPS Healthcare



Asma Omar Mohammed Muallemi

Dubai Municipality

Rahul Mishra

RAK Bank

Hind Ali Alloghani

Abu Dhabi Monitoring and
Controlling Centre

Abdulla Bader Al Sayari

Department of Health

Khaldoon Bargouthi

Mohamed Yousuf Naghi &
Brothers Group

Abdul Rahman

Omantel

Velmurugan S

Emaar

Ali Al Ameri

Abu Dhabi Retirement Pensions
and Benefits Fund (ADRPBF)

Abdulla Almarzooqi

Dubai Police

Khalid Othman Binahmad

STC Solutions, KSA

Hamad Al Balushi

Ajman Digital Government

Mohamed Abdulwahed Alajmani

Sharjah Customs

Hossam Abbas Barakat

Egypt Gas

Emad Maisari

Mubadala Investment Company

Shishir Deshpande

Alec

Hisham Mohamed Ali Ibrahim

Emirates NBD - Egypt

Abdul Rahman Shelleh

Al Dhafrah Region Municipality

Soney Paul Bahanan

NMC Healthcare Ltd.



tahawultech.com

FUTURE SECURITY AWARDS 2021



Fortinet
Best Network Security Vendor



Rackspace Technology
Best Managed Cloud Provider



Seclore
Best Data Protection Vendor



Hikvision
Best AI Security Vendor



ESET Middle East
Best SMB Endpoint Security Vendor



Help AG
Best Managed Detection and Response Service Provider



LinkShadow
Security Analytics Platform of the Year



Huawei Middle East
Best 5G Security Vendor



Sophos
Best Endpoint Security Vendor



Raqmiyat
Best Encryption Vendor



Ring
Best Smart Home Security Vendor



Mimecast
Best Email Security Vendor



Starlink
Best Security VAD



Help AG
Best Managed Security Services Provider



Protiviti
Best Security Consulting Services Partner



D-Link
Best Cloud Networking Vendor



Micro Focus
Best Cloud Security Vendor



Infobip
Best Digitalisation & Cybersecurity Provider



Virsec
Emerging Security Vendor of the Year



A PANEL DISCUSSION ON LEADERSHIP & THE CHANGING SECURITY DIALOGUE WAS HELD AS PART OF THE CISO 50& FUTURE SECURITY AWARDS HOSTED BY CPI LAST MONTH. WE BRING YOU A REPORT.

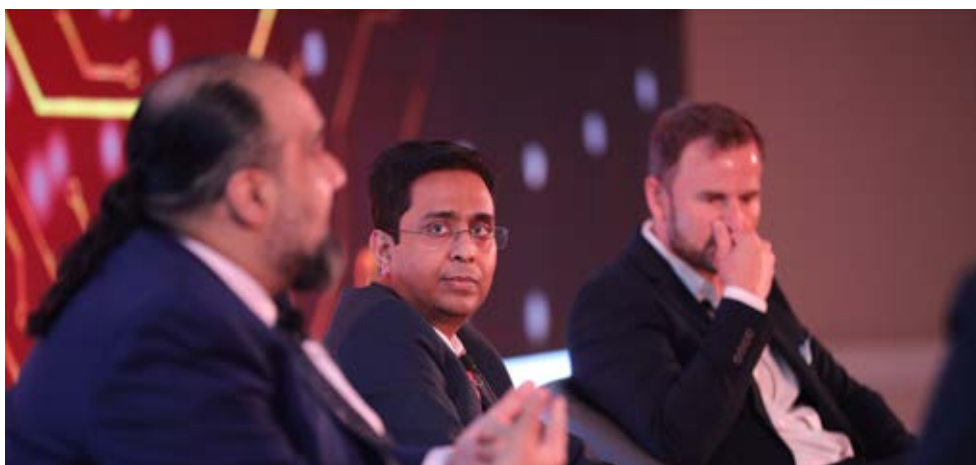
Four of the leading security decision makers in the region got together to debate the changing role of security leadership in the context of a rapidly evolving threat and security landscape. Moderated by **Anita Joseph**, editor, Security Middle East & Reseller Middle East, the discussion brought together **Mohamed Kamel**, customer success manager at Seclore Middle East, **Ahmed Diab**, senior sales director at StarLink, **Ranjan Sinha**, managing director at Protiviti and **Nicolai Solling**, CTO at Help AG, to explore the expanding role of CISOs and CIOs within an increasingly complicated cybersecurity landscape.

2021 can be called the Year of Transformation. It is the year in which companies, both large and small, have accelerated their digital transformation journey in order to ensure continuity of business operations and stay relevant

for customers. IT teams and their leaders are being faced with a sudden deluge of demands to execute the impossible in a short period of time.

As a result, the conversation around security is front and center. So much so that it's become top priority for business leaders as the world prepares to recover from the damages of 2020. This puts the Chief Information Security Officer (CISO) and other security professionals in the hot seat at every conversation — from the weekly IT department stand-up to the quarterly board meetings.

Introducing the transformational CISO/security professional: The leader who takes charge of an IT-focused organisation through a time of transformation. So, what are the challenges that today's CISO/security leaders face? How can they lead from the front and ensure that security is top priority while implementing new technology? Above all, how can they



ensure that the actions of today can bring about a safe and cyber threat-free world tomorrow? These questions formed the crux of the panel discussion.

All the panelists agreed that the role of the new-age CISO and other security decision makers brings with it its own challenges and pain points. "The new technologies that are coming into the picture-like IoT, blockchain and cloud-are putting increased pressure on the role of the CISOs and CIOs," said Mohammed Kamel. "However, in my opinion, I still believe that human error and lack of awareness of cybersecurity risks is the main challenge for any decision maker/CISO," he added.

According to Ahmed Diab, "the main challenge lies internally within an organisation, where the other departments and functions fail to understand the role of the CISO and how early on CISOs should be engaged with the business plan and goals of

the company. The budgets and the cost reductions that CISOs may face, especially post the pandemic, as well as the talent gap that currently exists, are the other challenges that decision makers face."

Ranjan Sinha said the main challenge faced by CISOs today was to "act as

"WE'RE GETTING TO A SPACE WHERE CISOS WILL HAVE TO START THINKING ABOUT WHAT IS APPROPRIATE TO HANDLE INTERNALLY WITHIN THEIR ORGANISATION AND WHAT THEY SHOULD RELY ON PARTNERS TO DO."

enablers rather than as inhibitors to the growth of the company. Many a time, CISOs are being branded as inhibitors where they actually can be enablers, and this is a huge cultural change that may be required."

Nicolai Solling was of the opinion that while cyber attackers are becoming better and better at what they do, more persistent and well-funded, we have CISOs who are being asked to do more with less, which resulted in a conflict between the two. "Also, with attackers being as professional as they are today, we have to look back and review whether we are actually able to deliver those services internally in our organisations. We're also getting to a space where CISOs will have to start thinking about what is appropriate to handle internally within their organisation and what should they rely on partners to do, so that we can let the professionals defend against the professionals."

The panelists also said there should be a bigger role for CISOs in business planning and business strategy and that security has to be the underlying pillar of all the infrastructure and resilience frameworks that organisations create, in order to ensure a safer and more secure world tomorrow. The discussion came to a close with the realisation that while the challenges facing CISOs are real and demanding, the right kind of leadership-futuristic and forward thinking-will help overcome these problems as we step into a new, "all-digital" era. 📌

LOOKING BEYOND DATA CLASSIFICATION

A ROUNDTABLE HOSTED BY CPI MEDIA GROUP AND SECLORE DISCUSSED WAYS TO NAVIGATE THE DLP/CLASSIFICATION/DRM/ ENCRYPTION LANDSCAPE FOR GREATER COMPLIANCE AND SECURITY.

Data protection is quickly becoming an impossible goal with the number of collaboration applications, devices, networks, and cloud services being used, increasing constantly. Interestingly, data-centric security technologies like DLP, Encryption and Classification have been around for some time but have taken a lot of time and resources to deploy.

The roundtable brought together industry experts-Eric Gayet, head of information security functions at Majid Al Futtaim Global Solutions, Harsh Daftary, lead security architect at Emirates NBD, Darko Mihajlovski, information & cybersecurity consultant at Deem Finance, Ismail Jani, manager, Information Security at Engineering Office and Shaik Sabir, head of unit, information technology section, Department of Finance- to debate the pros and cons of data-centric security technologies and also explore how automation is changing the landscape in data-centric security deployments.

The session was moderated by Vishal Gupta, CEO of Seclore, an IIT Bombay (Electrical Engineering) graduate and a specialist in biometric security systems.

Seclore is the leading player in the data centric security platform space and Vishal has led the company from founding to presently having 2,000+ enterprise customers in more than 29 countries. Vishal is also an active participant in physics activities and is an active sports person, a keen blogger on information

“THE DISCOVERY OF DATA OR THE CLASSIFICATION OF DATA ARE JUST MEANS TO AN END- DATA PROTECTION INITIATIVES WORK BEST WHEN THEY KEEP THE FINAL OBJECTIVE OF PROTECTING DATA AS THE GOAL, AND NEITHER DISCOVERY NOR CLASSIFICATION ARE HELPING TO ACHIEVE THAT END OBJECTIVE.”

security solutions and an intrepid speaker at various information security forums.

The main question driving the debate was whether the data-centric security technologies have actually delivered on their promise- and if not, what are the some of the biggest challenges in this value delivery process?

Eric Gayet stressed the need to revamp the process side of organisations and enhance awareness among people. “From my perspective, yes, technologies have delivered on the promise-not only to support the security strategy and agenda we all have for the organisation, but also tackle the multiple compliance requirements that we need to align and be compliant with. In terms of the challenges, there is a basic principle that we will all agree with-people, process and technology. I will say technologies are quite mature today, however, in most of the organisations, the process side, the awareness and understanding among people of the risk, the objectives and the reason for doing what we do, is still an area where we have a lot on the plate, lots to do.”

According to Harsh Daftary, sometimes the products themselves are faulty. “If you look at the satisfaction score, out of 100, we are sometimes only 60 percent satisfied with a product and we’ve shifted between products mid-way. We’ve discovered that classification & DLP do not fit each other because there is no unified labelling between the two, and for this, we had to bring in a separate plug-in-the kind of engineering we’ve had to do was crazy. In fact, it was not only about the quality, the products themselves have security holes in them.”

Darko Mihajlovski said it was not just about the maturity of the organisation or the awareness of its people, but also the fact that sometimes, being too professional about cybersecurity can get too noisy for organisations and they don’t want to accept that. “So, education and awareness among all the ranks of the organisation, but also, whenever you want



Vishal Gupta



Shaik Sabir



Harsh Daftary



Eric Gayet



Darko Mihajlovski



Ismail Jani

to initiate data classification, it should come from the top and the CISOs should take over," he pointed out.

For Ismail Jani, a major aspect about all of this centred around bringing a cultural change within an organisation. "This can be achieved only when you interact with every department, every business line, and consider everyone a stakeholder. Also, with security teams, we'll have to get a buy-in from everybody, include all business processes and business rules in your classification, and have a simple classification system like 1, 2, 3 and 4 where most of the classifications can fit and people can identify easily."

Vishal said the biggest challenge is all about end-user involvement and that all organisations must keep the final objective of data protection in mind. "The discovery of data or the classification of data are just means to an end—data

protection initiatives work best when they keep the final objective of protecting data as the goal, and neither discovery nor classification are helping to achieve that end objective. The challenge is also that these data discovery and classification projects never come to an end—you have to go on and on and the actual step of data protection never happens. Enterprises have so much data, so many people, that these projects never end."

Vishal also emphasised the need to look past data discovery and data classification as the final goal. "There is an emerging class of technologies that are data protection platforms. What these platforms do is that they effectively integrate information coming in from the discovery systems, the DLP systems, the classification systems, a rights management or an encryption system. Then you have a step after this, which is data-centric monitoring. You don't only

want to protect, you also want to monitor what happens to the data after you've protected it. These data-centric security platforms are unifying platforms that takes care of all the different challenges. All of the uncertainties get abstracted out. We need to make sure that in our data protection journey, we keep the final objective in mind and don't treat data discovery and classification as the final goal, because it is not."

The panelists agreed that while there are many pain points, the ultimate goal of protecting data is what all organisations need to have in mind and to do that effectively, organisations need to look at the various automation frameworks that can analyse a piece of data, figure out the policy that should govern this data and then directly implement the policy, so that the whole, cumbersome discovery-classification process, can in many cases, be bypassed completely. 🙌

INDUSTRIAL CYBERSECURITY: HOW TO PROTECT YOUR ASSETS IN THE DIGITAL TRANSFORMATION AGE

AS THE INDUSTRIAL WORLD BECOMES EVER MORE CONNECTED AND COMPLEX, THE NEED TO EMBED PERVASIVE CYBERSECURITY POLICIES IS PARAMOUNT, SAYS **TIM GRIEVESON**, CHIEF INFORMATION SECURITY OFFICER, AVEVA.

In an age of rapid digitisation and always-on connectivity, the industrial landscape has never been more ready for transformation. Post-pandemic, companies have learned radical lessons about how to run and optimise systems in unpredictable operational times. As such, global organisations have been compelled take decisive action by putting technology at the very heart of their business processes. Cybersecurity is a key business differential in ensuring these operations are secure and resilient.

With the rapid and significant need to enable remote work and team collaboration, software solutions like Cloud, Edge and IoT can pave the way for improved business performance and procedures. But with great opportunities also come challenges. As such, more complex industry technology solutions demand a heightened focus on cybersecurity and securely enabling the work-from-anywhere culture.

Industrial risks

According to global cybersecurity analysts,

industrial systems are still not yet sufficiently protected against the new and multi-faceted risks of digital transformation, despite being susceptible to increasing risks for many years. In order to be effective, company cybersecurity policies must proactively and holistically pervade the entire organisation. A balance should also be struck between mitigating risks and enabling new business initiatives. What's more, it's imperative that companies focus not only on training staff but also on selecting appropriate and best-of-breed technology partners who build security into the ecosystem of how they operate, as opposed to charging extra or having security as an add-on.

Key security considerations

Industrial businesses that embrace transformation and have a holistic view of cybersecurity are benefitting from diverse technology ecosystem development, including connected devices, edge control, apps, analytics and cloud services, which are enhancing business performance at an unprecedented pace.

It's vital that your organisation's approach to security is part of the organisational culture – using components that meet recognised standards and include encryption by default. Security must be integral to the design of any process or operation and fundamentally baked into the services that support the operation of your systems and business objectives.

Company checklist

The tsunami of risks focused on operating technology (OT) ranges from the exposure of intellectual property and lost production systems or data to serious fines and reputational loss. Cybersecurity is a multi-faceted discipline requiring a proactive approach across the business. For your business to be best prepared against threats, it's important to consider the following elements:

People

Ensure you invest in your people by providing relevant and timely security training for staff, contractors and third parties, which not only supports your organisation's objectives but



Tim Grieveson

can be used in personal digital lives too. It's essential to engage all your employees as active cybersecurity ambassadors by educating them on identification, prioritisation and understanding the changing security landscape including dangers of malware, phishing, unofficial USBs and social media oversharing so they can behave and act accordingly.

Network

It's vital to maintain a unidirectional gateway between IT and OT systems, as well as running continuous vulnerability assessments and installing anti-malware solutions for industrial end points, as well as your corporate and lab environments.

Partners

Select vendors that will partner with you to protect critical data and understand your security, legal principles and privacy policies. Determine where and how data will be collected, used and stored. Ensure partners include security as a core component of their service offering as opposed to an optional extra. Ensure they take shared responsibility for good cyber hygiene and are transparent on what they can and cannot do to support your business.

Processes

It's important to build a culture of cross department buy-in across management, IT, security and business operational teams

for cybersecurity processes. In addition, you should develop your cybersecurity program to ensure continual improvement ensuring you build in findings from regular audits and vulnerability assessments to ensure systematic risk burn down and capability improvement.

Devices

Ensure you change your IoT device passwords from the factory default; extend your security and password policies to mobile devices; and conduct regular intrusion testing and anomaly detection on all devices. Never assume your devices are safe and always validate and include them in your security assessment strategy.

Vendor checklist

When considering your cybersecurity needs, choosing the right partner is crucial. Software vendors play a key part in your cyber defence strategy. When considering a cloud or IoT partner, here are some key questions to consider:

Physical security

Where are their cloud services physically deployed? Where will my data actually reside? Where and how will my data be captured, stored and used?

Data security

How is your information protected – at rest and in motion?

Does your vendor support unidirectional data transfer? How does your supplier deal with network outages?

Application security

How do they handle authentication, authorisation and account management? What is their approach to identity and access management (IAM)? Are they using a recognised secure development framework? What is their response to identification and remediation of known and unknown vulnerabilities?

Continuous monitoring and improvement

Do they have proactive monitoring and active security policies in place? Can they identify abnormal behavior and catch anomalous activity? What procedures are there to detect and isolate suspicious activity online? Do they use threat information derived from monitoring to continually improve security controls and techniques?

Security assessments

Do they have a proactive program of internal and external security audits? How do they deal with ongoing compliance with regulations, such as GDPR? Do they have a published security statement that you can read? When you detect vulnerabilities how do they disclose them and how promptly do they remediate?

Staff

How do you vet and train your staff? Do your staff hold relevant security certifications and experience – and do they share this information with you? Do your staff use third-parties as part of the service delivery and how do they ensure compliance with your security principles? By including these basic cyber stages in your security strategy, you will take the first steps towards a complete protection strategy. In today's world of ever more complex cyber threats, a comprehensive security strategy – covering all the basics – is no less than critical for protecting your digital and physical assets. 📌

“ACCORDING TO GLOBAL CYBERSECURITY ANALYSTS, INDUSTRIAL SYSTEMS ARE STILL NOT YET SUFFICIENTLY PROTECTED AGAINST THE NEW AND MULTI-FACETED RISKS OF DIGITAL TRANSFORMATION, DESPITE BEING SUSCEPTIBLE TO INCREASING RISKS FOR MANY YEARS.”

ACRONIS CYBER PROTECT HOME OFFICE: OFFERING COMPREHENSIVE DATA PROTECTION AND CYBERSECURITY

THE AWARD-WINNING PRODUCT (FORMERLY ACRONIS TRUE IMAGE) PROVIDES INDIVIDUALS WITH COMPREHENSIVE PROTECTION AGAINST ALL THREATS — FROM DISK FAILURES TO CYBERATTACKS.

Acronis, the global leader in cyber protection, has released the newly-rebranded Acronis Cyber Protect Home Office (formerly Acronis True Image.) This new name for the company's flagship personal solution reflects its evolution from data and system backup software to a solution that delivers complete cyber protection — next-generation anti-malware, best-in-breed backup, and easy management, all-in-one integrated tool.

Cyber protection

The need for both effective data protection and cybersecurity has become dominant in daily life. Businesses rely on the continuous availability and integrity of their data, while individuals

around the world send and receive large volumes of sensitive information over remote connections. Cybercriminals, in response, have stepped up the scale and complexity of their attacks — and with advances in the automation of these threats, no one is “too small to target.”

Recognising the evolving challenges of data protection, Acronis has been advancing its solutions since 2017 to meet the latest challenges. When ransomware threats began targeting file backups directly, the company became the first to integrate anti-ransomware defenses into a personal backup solution. In 2021, Acronis continued to expand its cybersecurity focus, adding capabilities that include threat-agnostic anti-malware, cryptojacking protection, and web filtering. The solution evolved

from a backup one to a completely personal cyber protection solution, safeguarding not only backups but devices as well.

Acronis' success with these efforts has not gone unnoticed, earning Editor's Choice awards from both PCWorld and PCMag. PCWorld called it “an all-encompassing tragedy-prevention solution.” When evaluated by independent security research lab AV-TEST, the integration of data backup and advanced cybersecurity successfully detected and blocked 100% of cyberattacks.

Protection for everybody

Acronis Cyber Protect Home Office (formerly Acronis True Image) incorporates a number of capabilities



to counter modern cyberthreats and ensure complete data protection. The unique integration of cybersecurity and backup into a single solution not only makes protection simpler and more affordable, but also delivers advanced capabilities that standalone solutions cannot — such as the automatic restoration of any data damaged during a ransomware attack.

Its advanced anti-malware is proven to detect and stop the latest cyberthreats in real-time, including zero-day attacks that have never been seen before. Protection is extended across popular software, including video conferencing applications like Zoom and Microsoft Teams, preventing attackers from accessing data in-transit.

“The past two years have changed the

industry landscape for good, no user is too small to be targeted anymore” said Candid Wuest, Acronis VP of Cyber Protection Research. “The unique quality of our corporate solutions is the integrated cyber protection – combining cybersecurity and backup is the only

**RECOGNISING
THE EVOLVING
CHALLENGES OF DATA
PROTECTION, ACRONIS
HAS BEEN ADVANCING
ITS SOLUTIONS SINCE
2017 TO MEET THE
LATEST CHALLENGES.**

way to keep your critical data truly protected. Now we offer Acronis Cyber Protect Home Office – to protect every individual and home office, and keep the world going despite the challenges of the remote work and distributed IT infrastructure.”

To learn more about the cybersecurity and data protection capabilities that Acronis Cyber Protect Home Office enables for individuals such as home users, remote workers, freelancers, and at-home students, visit the official page.

About Acronis

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

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,700 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages. 🇮🇸

CYBERSECURITY CONTROLS TO STOP RANSOMWARE

RAYMOND POMPON, DIRECTOR OF F5 LABS, ON RANSOMWARE AND WHAT CAN BE DONE TO PREVENT THIS.

F5 Labs' 2021 Application Protection report shows that ransomware was a factor in about 30% of U.S. breaches in 2020. This trend is also playing out to varying degrees globally. When we look at the breach analyses, some of the most important controls were user account management, network segmentation, and data backup. The challenge is how to best implement them.

Ransomware defense no. 1: user account management

A significant percentage of attackers log into systems to hack them. They guess, steal and phish passwords. Indeed, historically speaking, passwords provide poor protection. Here's how we can do better:

Enable multifactor authentication on everything you can

Best practices, and some compliance regulations, indicate the use of multifactor authentication (MFA) on all systems holding critical data. If you can't apply MFA to everything, then prioritise. First, all administrative accounts should use MFA. As a major attack vector for ransomware, remote access is the next priority. Given all

the critical data people leave in email and that most major email platforms support MFA, adding it to end-user email is the next priority.

Implement a robust password policy

Until you can get to 100% MFA for all access (hint: look for single sign-on tools to help here), we advise looking into the following measures (based on the NIST Digital Identity Guidelines):

- Make your password policies user-friendly.
- Regularly check passwords against a dictionary of default, stolen, and well-known passwords.
- Never use hints for password resets.
- Use long passwords.
- Avoid arbitrary password rotations.
- Lock or remove unnecessary credentials.

Limit administrative access

Strong account management means applying the principle of least privilege. The key priority is to limit administrative access. Unless you're an IT shop of one person that works 24/7, divide the responsibilities by region, time zone, or system function. Another powerful technique is to separate the system administrator accounts from their

day-to-day user accounts. Admins should use a nonprivileged account for things like reading email, surfing the web, and accessing applications. Then, when they need to perform IT administration, they switch accounts or elevate their privileges. This way, if an admin accidentally clicks on a phishing email with ransomware, it won't wipe out the entire network. Many of these restriction capabilities are configurable within most operating systems.

The same approach applies to service accounts. These are the often invisible accounts that are tied to running applications. These services are ripe for attacker takeover. Associated accounts should restrict rights to only those necessary to run the service. Web servers need rights to their own service and the file directories, not an entire box or the entire network. Using a generic full admin account as a service account is a disaster waiting to happen. Operating systems have some built-in functions to restrict these service accounts, disallowing human interactive logins and tying them only to the servers and services they are supposed to function on.

In some systems, you can restrict service account privilege domains as well. For example, you can set up a backup server to have read-only access to the main domain, so it can copy files for backup. Restores can be done under a different account or manually with a system administrator.



Raymond Pompon

Monitor access

All user accounts should be logged for audit purposes in a way that prevents tampering. Attackers will try to erase their tracks, so your monitoring system should sound the alarm if it detects logs being deleted or they stop coming in. It's also prudent to have the system automatically raise an alert when a system administrator account is created. This should be a rare enough event that false positives are manageable. It is also important to review general user accounts against personnel records to ensure only the right people continue to have access. Lastly, because of the prevalence of brute force and credential stuffing attacks, create alerts for large numbers of login failures.

Ransomware defense no. 2: network segmentation

Firewalls can limit infections to specific segments of users, systems, or levels of trust. Virtual LANs, which run on managed switches, can also be a useful fallback if internal firewalls are unfeasible. This is essentially least privilege at a network level.

Segment trust boundaries

Worried about supply chain compromise of your management tools? Set up default deny policies with firewall rules controlling the management servers. Then configure only the specific connections and ports necessary for remote management

capabilities to the specific managed system addresses. Note that a remote management system can have Internet access or internal network access but not both simultaneously. Make it harder for an Internet attacker to remote control a server in your environment. The same rule applies for administrative interfaces: limit their access with network rules.

Network traffic can be filtered wherever subnets of different trustworthiness connect to each other, such as wireless networks, remote access gateways, third-party connections, storage servers, Internet-of-Things devices, backup servers, developer systems, and user networks. Once again, apply least privilege and only allow the defined communication methods to the defined addresses.

Patch network infrastructure

The network devices and firewalls that manage network segmentation also need to be patched in a timely manner. Attackers will exploit those bugs and break through, so make sure to keep those devices up to date.

Ransomware defense no. 3: data backup

Once ransomware takes hold of your systems, it's best to delete everything and reload from scratch. Attackers know this and will corrupt backup systems as part of the ransomware attack. So, have complete, up-to-date backups, and protect them.

Use the 3-2-1 backup method

Use the 3-2-1 backup strategy. This means having three backups of your data, with two

copies on different media, and one offsite. Remember to back up everything, including system images, application software, and configurations. You can then rebuild servers and workstations, preferably using automation for speed and ease.

Test your complete restore process

Restore testing should include tests for completeness and speed. It's one thing to perform a test restore for a few files but another thing to restore hundreds of terabytes. In many cases, a complete restore process can take days to complete. Also, if you are backing up online – such as saving data to the cloud – check your bandwidth speed requirements and costs. Some cloud providers charge much more in transfer fees to download data from their cloud than to upload to it.

Use immutable backups

Most major cloud providers now offer immutable storage options, such as placing a software lock on a file when it's created. The lock can remain in place for weeks or months to ensure stored files cannot be altered. These locks can both protect against ransomware and meet compliance and legal requirements for tamperproof logs.

Defense in depth

Ransomware is a growing threat to our critical systems. Fortunately, a defense in depth strategy can prevail.

Ultimately, though, there is no cut-and-dried checklist on what controls and defenses to leverage. It will vary based on your organisation's business, technological infrastructure, culture, and relevant threats. The key is analysing and understanding the threats you face and the assets you care about, and then applying divergent but overlapping controls to remediate as much risk as you can. The good news is that a coordinated collection of useful but imperfect defenses is not only more effective than a single bulletproof control, it's a lot more attainable. 🛡️

“STRONG ACCOUNT MANAGEMENT MEANS APPLYING THE PRINCIPLE OF LEAST PRIVILEGE. THE KEY PRIORITY IS TO LIMIT ADMINISTRATIVE ACCESS.”

BEST OF NETAPP DELIVERED WITH THE BEST OF AWS



Anthony Lye

ANTHONY LYE, SVP & GM CLOUD DATA SERVICES AT NETAPP, DISCUSSES THE AMAZON FSX FOR NETAPP ONTAP SERVICE THAT MAKES IT EASY AND COST EFFECTIVE FOR BUSINESSES TO LAUNCH AND RUN SHARED STORAGE FOR WINDOWS AND LINUX WORKLOADS.

AWS have just announced the general availability of Amazon FSx for NetApp ONTAP, a native AWS managed service powered by NetApp ONTAP software and available around the world. This new AWS service makes it easy and cost effective for businesses to launch and run shared storage for Windows and Linux workloads, while offering NetApp's suite of enterprise-grade data services—all running in an AWS native experience.

For NetApp, this moment represents the culmination of years of hard work and continuous innovation bringing ONTAP to the cloud. Long trusted in the data center, we're now the first and only storage environment that is truly enabled for hybrid cloud and natively integrated into each of the major public cloud providers.

This innovative foundation enables IT operations to extend data centers and migrate enterprise applications like SAP, relational databases, and virtual machines to AWS. But that's just the beginning. We've progressively added a wide range of new cloud data services to help you back up, replicate, protect, and cache data while maintaining compliance. We empower you to successfully navigate the challenges of managing hybrid cloud infrastructure.

To the thousands of existing customers who know and love ONTAP from their data centers, Amazon FSx for NetApp ONTAP directly offers the full set of ONTAP features and APIs—all available on day 1. Besides managing ONTAP natively from the AWS Management Console or accessing APIs through AWS SDKs and the AWS Command Line Interface (CLI), you can easily add your AWS infrastructure to your NetApp Cloud Insights dashboard

“TO THE THOUSANDS OF EXISTING CUSTOMERS WHO KNOW AND LOVE ONTAP FROM THEIR DATA CENTERS, AMAZON FSX FOR NETAPP ONTAP DIRECTLY OFFERS THE FULL SET OF ONTAP FEATURES AND APIS—ALL AVAILABLE ON DAY ONE.”

and use NetApp Cloud Manager to orchestrate all your data and cloud services. And if you're a customer of Spot by NetApp, you can immediately tap into the power of Spot Storage, continually optimising storage and compute resources to cost-effectively match application needs for virtual machines and containers. At the risk of hyperbole, this is a real game changer.

This tight integration of ONTAP into the infrastructure of AWS allows both born-in-the-cloud companies and stalwarts of industry to seamlessly use NetApp's broader cloud portfolio. Any company—big or small, a department or a division, an integrator or an independent software vendor—can easily implement this technology. They'll get NetApp's powerful data services and applications combined with AWS-native APIs and rich services for launching, scaling, monitoring, and managing applications and workloads in AWS. Each of these services is designed to deliver immediate business value, whether in the form of cost efficiency, compliance, data protection, or performance.

There's a reason AWS chose NetApp. ONTAP provides fully-featured and high-performance shared storage for file and block workloads. Integrated with a wide range of enterprise-proven capabilities, ONTAP is the most efficient, resilient, and highest-performing data management software in the world. We make it easier and faster to build rich experiences and to manage data sets so you can migrate and run primary applications, extend on-premises infrastructure to the cloud for disaster recovery, build dev/test environments, back up data, burst and cache, and set the stage for stateful applications to run in containerised applications.

Depending on your business needs, FSx for ONTAP offers several options for protecting your data. NetApp Cloud Backup (integrated with FSx for ONTAP backups) delivers cost-effective backup and restore capabilities for cloud and on-premises ONTAP data. You can drastically reduce backup times and instantly restore data from in-place zero-impact NetApp Snapshot™ copies if data loss, ransomware, or data inconsistency occurs. The NetApp SnapMirror® feature provides highly available and efficient replication of data copies, including support for multiple Availability Zones and cross-region disaster recovery to protect and test against site outages without disruption. The NetApp FlexClone® feature delivers fast, space-efficient copies and fully supports block-level “forever” replication.

For nearly a decade, NetApp and AWS engineers have worked together to create industry-leading cloud services. Hats off to all the teams who made this achievement possible. We are so excited to begin writing this new verse of innovation with AWS customers. 🙌



→ **TO DETERMINE THE SCOPE AND IMPACT OF AN ATTACK, ORGANISATIONS FIRST NEED TO IDENTIFY THEIR HIGHEST PRIORITY ASSETS.**

CAN ORGANISATIONS BE PREPARED FOR A CYBERATTACK?

HARISH CHIB, VICE-PRESIDENT MIDDLE EAST & AFRICA AT SOPHOS, ON HOW TO CREATE AN EFFECTIVE CYBERSECURITY INCIDENT RESPONSE PLAN.

Believe it or not, ransomware and other cyberattacks are the last sign an adversary has breached an organisation's network. In fact, when it's obvious that a business has been victimized by an attack, it typically means cybercriminals have been lurking for days, if not months. The question is, if cyberattacks take a while to execute, can organisations be prepared and act in real time to minimise the damage of cyberattacks?

The best way forward for businesses is to have a structured Incident Response



Harish Chib

Plan, so they can act as fast as possible when under an active attack.

Sophos recommends the following 10 steps to create an effective cybersecurity incident response plan, based on the real-world experiences of its Sophos Managed Threat Response and Sophos Rapid Response teams, who have tens of thousands of hours of experience when it comes to dealing with cyberattacks.

10 STEPS TO CREATE AN EFFECTIVE CYBERSECURITY INCIDENT RESPONSE PLAN

1. Determine key stakeholders

Properly planning for a potential incident is not the sole responsibility of security teams. In fact, an incident will likely impact almost every department in an organisation, especially if the incident turns into a full-scale breach. To properly coordinate a response, organisations must first determine who should be involved. This often includes representation from senior management, security, IT, legal, and public relations.

2. Identify critical assets

To determine the scope and impact of an attack, organisations first need to identify their highest priority assets. Mapping out highest priority assets will not only help determine a protection strategy, but will also make it much easier to determine the scope and impact of an attack.

3. Run tabletop exercises

Incident response is like many other disciplines – practice makes perfect. While it is difficult to fully replicate the intense pressure, the teams will experience during a potential breach, practice exercises ensure a more tightly coordinated and effective response when a real situation occurs. It is important to not only run technical tabletop exercises, but also broader exercises that include the various business stakeholders previously identified.

4. Deploy protection tools

The best way to deal with an incident is to protect against it in the first place. Organisations should ensure they are using the appropriate endpoint, network, server, cloud, mobile, and email protection.

5. Ensure maximum visibility

Without the proper visibility into what is happening during an attack, organisations will struggle to respond appropriately. Before an attack occurs, IT and security teams should ensure they can understand the scope and impact of an attack, including determining adversary entry points and points of persistence.

6. Implement access control

Attackers can leverage weak access control to infiltrate an organisation's defenses and escalate privileges. Organisations should regularly ensure that they have the proper controls in place to establish access control.

7. Invest in investigation tools

In addition to ensuring the necessary visibility, organisations should invest in tools that provide the necessary context during an investigation.

Some of the most common tools used for incident response include Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR), which allows organisations to hunt across their environment to detect indicators of compromise (IOCs) and indicators of attack (IOA).

8. Establish response actions

Detecting an attack is only part of the process. To properly respond to an attack, IT and security teams need to ensure they can conduct a wide range of remedial actions to disrupt and neutralise an attacker.

9. Conduct awareness training

While no training program will ever be 100% effective against a determined adversary, education programs (i.e. phishing awareness) help reduce the risk level and limit the number of alerts security teams need to respond to.

10. Hire a managed security service

Many organisations are not equipped to handle incidents on their own. Swift and effective response requires experienced security operators. To ensure this, organisations should consider working with an outside resource such as a Managed Detection and Response (MDR) provider.

To sum up, when a cybersecurity incident strikes, time is of the essence. Having a well-prepared, well-understood response plan that all key parties can immediately put into action will dramatically reduce the impact of an attack on an organisation. 🧑‍💻

IT'S TIME TO BRING IN THE CYBERSECURITY EXPERTS

SUNIL PAUL, CO-FOUNDER & MANAGING DIRECTOR AT FINESSE, DISCUSSES HOW MANAGED SERVICE PROVIDERS CAN HELP, AS REMOTE WORK MODELS INCREASINGLY BECOME POPULAR AND THE PUSH TOWARDS DIGITAL TRANSFORMATION INTENSIFIES.



Sunil Paul

2021 has been a busy year for cybersecurity professionals so far. With global security incidents such as the Colonial Pipeline and Kaseya cyber-attacks, as well as the Microsoft Exchange data breach, business leaders are recognising that cybersecurity can no longer take a back seat.

As remote work models increasingly become popular and the push towards digital transformation intensifies, customers have their hands full as they step up their environments and workloads to the cloud, train staff to operate with new technologies, and simultaneously ensure productivity and profitability. However, having dedicated personnel and resources to constantly monitor the threat landscape can prove

to be an expensive and arduous task. This is where managed security services can come to the rescue.

There are several benefits to outsourcing your cybersecurity to a third party, the biggest one being cost savings and unparalleled expertise. In addition, enterprises can save on expenses across different areas such as salaries for dedicated in-house cybersecurity talent, office space, trainings, and so on, which would otherwise require deep pockets.

Managed Security Services Providers (MSSPs) offer a competitive edge to customers as they house the latest cybersecurity solutions and technologies with in-depth knowledge about the evolving threat landscape. These unique skillsets allow for early detection of any security vulnerabilities, continuous monitoring, and immediate solutions. With business environments becoming digitally advanced and more connected than ever before, threat actors are having a field day. In fact, a report by research firm Cybersecurity Ventures revealed that cybercrime will cost companies globally an estimated \$10.5 trillion annually by 2025, up from \$3 trillion in 2015. This would mean enterprises must invest heavily into cybersecurity tech and talent to keep their ships afloat. Offering 24/7 support, MSSPs can help take this load off so that customers can focus on their core business objectives. What's more – MSSPs can also custom-built cybersecurity solutions catering to a customer's specific business requirements and budgets.

By contracting an MSSP, organisations have access to enterprise-grade holistic cybersecurity hubs. These shared Security Operation Centers (SOC) allow companies of any size to leverage advantages such as flexibility, scalability, relevant skillsets, 24/7 support, and so on, without having to commit significantly financiall.

There is no debate that MSSPs are the need of the hour in today's cybersecurity climate. At the onset of the COVID-19 pandemic, the region has experienced an alarming increase in cybercrime. A Kaspersky study reported that in the Middle East alone, there were 2.57 million phishing attacks over a period of just three months in 2020. According to the security leader, both UAE and Saudi Arabia saw a significant increase in phishing attacks. And it's not just phishing – from ransomware, malware, DDoS, data breaches to insider threats – the region has been earmarked by cyber perpetrators. Cybersecurity vendor Mimecast's 'The State of Email Security' report revealed that 78% of organisations in the UAE indicated they had been impacted by ransomware in 2020, a big increase from 66% in 2019.

Customers are realising that these are not just random figures or statistics with recent news of local entities such as Moorfields Eye Hospital Dubai, confirming cyber-attacks. These reports close to home are further driving organisations to rely on MSSPs for their end-to-end security needs. This is further reinforced in a Kaspersky study earlier this year, which found that around 70 percent of organisations plan to outsource security to an MSSP or an MSP over the next 12 months.

Maintaining an effective cybersecurity program can often be a challenging undertaking for any organisation. It also puts immense pressure on security leaders. However, it is important for them to know that they are not alone. Partnering with MSSPs like Finesse can enable them with the right capabilities, talents, and tools in the continuous battle against cyber threat actors. 🧑‍💻

17-21 OCT 2021
DUBAI WORLD TRADE CENTRE

GITEX
TECHNOLOGY
WEEK

ai
عالم الذكاء الاصطناعي
EVERYTHING

GF
GITEX FUTURE STARS

Fintech
SURGE.
مبتكرات سيرج

FUTURE
BLOCKCHAIN
SUMMIT
قمّة مستقبل البلوك تشين

ماركتنغ مانيا
Marketing
Mania

17-20 OCT 2021

**WHERE BUSINESS,
INNOVATION,
AND THE FUTURE
WILL BE DECIDED**

**140 COUNTRIES PRESENTING THEIR TECHNOLOGIES,
MAKE SURE YOU'RE THERE TOO**

SECURE YOUR SPACE NOW: marketing@gitex.com

#GITEX2021
GITEX.COM

Gold Sponsor

HUAWEI
5G Innovation Partner

Bronze Sponsor

CISCO

VIP Majlis Sponsor

midis
GROUP

Platinum Sponsor

NEOM
نيم

Conference Sponsor

TeamViewer

Headline Sponsor
Xlabs

APTEC

Headline Sponsor
Xlabs

Bitdefender

Supporting
Sponsor Xlabs

OBRELA
SECURITY INDUSTRIES

Supported by

AVAYA

vmware

Honeywell

Hisense

Red Hat

Organised By

مركز دبي للتجارة العالمية
DUBAI WORLD TRADE CENTRE

mimecast®

The State of Brand Protection 2021



MEMBER LOGIN

Username

Password

Login Now

☐ Remember me

[Forgot password?](#)

[Create account](#)

A new front opens up in the war of brand safety

Did you know that **40%** of consumers don't hesitate to click on links in emails from their favorite brands?

Download our **State of Brand Protection** report to become the master of your brand domain and learn how to keep your brand safe from #cybersecurity threats.



www.mimecast.com/state-of-brand-protection

NASDAQ: MIME