ADVISOR

COMMVAULT NETWITNESS FIDELIS

ENHANCING CYBER RESILIENCE

JOHN DOLEY, REGIONAL SALES DIRECTOR - META WHO LEADS THE ACCESS MANAGEMENT SOLUTIONS AT THALES TELLS ANITA JOSEPH, EDITOR, SECURITY ADVISOR MIDDLE EAST, THAT IT IS IMPORTANT TO LOOK FOR A SOLUTION THAT CAN PROTECT AND INTEGRATE WITH ON PREMISES AND CLOUD SERVICES TO HELP REDUCE COMPLEXITY AND HELP WITH REGULATORY COMPLIANCE AT THE SAME TIME. SPECIAL REPORT SECLORE





Unlimited Devices. Unlimited Networks. Unlimited Possibilities.

Control your network remotely without going onsite and see all your network locations, devices & clients with real-time data from a single view.

A Ouk Hits Corporation -					Q and		
have been for the	1 ma					•	
Office Build	ding 3, Floor 5			-			
Come Come							
Name And Make 10	-						
		7					
Maellor							
Batas			April Mail Said	sharff Their off	Sec.		
Colors 545740							
2240 A.M. AM. 34		1000 Jane	1999. 1999.1.1	100 1000	12.04		
Conservation							
Otine		Manager .					
		Medium					

LINKSYS



1300AC WiFi 5 MU-MIMO Cloud Managed Wireless Access Point LAPAC1300C



Outdoor 1300AC WiFi 5 MU-MIMO Cloud Managed Wireless Access Point LAPAC1300CE

Key Features

- Free Cloud-Native Centralised Management
- Multi-role platform built for managed service providers
- Zero Touch deployment

- Batch remote firmware upgrade
- Simple and responsive User Interface
- Cloud Hosted Captive Portal Splash Page

Linksys Managed Gigabit PoE+ Switches

Designed for security and speed, Linksys Managed Gigabit PoE+ Switches provide a business-class network you can grow on. LGS310MPC 8-Port: 133 Watt LGS328MPC 24-Port: 500 Watt LGS352MPC 48-Port: 885 Watt

Key Features

- High PoE+ Power Budgets
- Advanced Network Security and QoS
- Static Routing and IPv6 support



CONTENTS







ENCHANCING CYBER RESILIENCE

John Doley, Regional Sales Director - META who leads the Access Management Solutions at Thales tells Anita Joseph, Editor, Security Advisor Middle East, that it is important to look for a solution that can protect and integrate with on premises and cloud services to help reduce complexity and help with regulatory compliance at the same time.

06 NEWS We bring you the latest news roundup from the security industry.

INTERVIEW

Echo Zhao, Product Manager at Hikvision, about their cutting-edge products and solutions.

28

Keiron Holyome, Vice President – UKI, Middle East and Africa, about how Blackberry's strategy of preventing pre-execution malware helps organizations in the region grow their business in a safe and secure manner.



Martin Sutherland, General Manager, NetWitness, on the need for foresight about potential security breaches.



Bedata ready.

Commvault is a worldwide leader in delivering data readiness. Our intelligent data management solutions work on-prem and in the cloud, allowing you to store, protect, optimize, and use your data. Always.

commvault.com



EDITORIAL



Talk to us: E-mail: anita.joseph@ cpimediagroup.com

> Anita Joseph Editor

EVENTS



ROUNDING UP THE YEAR

We're in the final months of 2021 and

what a year it's been! As far as the security landscape was concerned, it was particularly momentous and challenging: As the world shifted online en masse, security concerns mounted and most companies were faced with the daunting task of managing and securing massive amounts of data. There was a sudden scramble to implement stronger security frameworks and keep up with the sudden slew of cyber-attacks, especially ransomware

The November issue of this magazine focuses on these threats and how different companies are ensuring the safety and security of their customers.

Our cover story with John Doley, Regional Sales Director – CPL at Thales Group discusses the need to look for security solutions that can protect and integrate with on premises and cloud services to help reduce complexity and help with regulatory compliance at the same time.

We have a special interview with Keiron Holyome, Vice President – UKI, Middle East and Africa, on the changing cybersecurity landscape and how Blackberry's strategy of preventing preexecution malware helps organizations in the region grow their business in a safe and secure manner.

We also have detailed interviews with Ivan Dolensky (Senior Vice President -International Sales), Fidelis Cybersecurity, on the threatrisk landscape and the roadmap for the region and Shai Nuni, VP, Metallic EMEA at Commvault, about Metallic, a service that lets one back-up and restore data

> without having to install and maintain traditional backup software.

Not to be missed are conversations with Echo Zhao, Product Manager

at Hikvision, about their cutting-edge products and solutions and senior officials at Netwitness, about the cybersecurity landscape in the region.

In addition, we also have the regular news updates, insight and opinion columns and other important security developments you wouldn't want to miss.

So, enjoy this power packed issue, happy reading!



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

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

© 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.

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

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

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

Senior Sales Manager Sabita Miranda sabita.miranda@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.ioseph@cpimediagroup.com

Online Editor Daniel Shepherd daniel.shepherd@cpimediagroup.com DESIGN Senior Designer Analou Balbero analou.balbero@cpimediagroup.com

> DIGITAL SERVICES Web Developer Adarsh Snehajan

IT'S BEEN A Momentous year for The cybersecurity Industry.

THREATQUOTIENT LAUNCHES THREATQ V5 TO SUPPORT SOC OF THE FUTURE WITH KEY DATA MANAGEMENT CAPABILITIES

ThreatQuotient, a leading security

operations platform innovator, has

announced v5 of the ThreatQ platform, launching capabilities needed today to support the security operations center (SOC) of the future, where data is the foundation ThreatQ's newest features include a unique DataLing Engine for connecting disparate systems and sources to enable extended detection and response (XDR), Smart Collections for driving automation, and an enhanced ThreatQ Data Exchange for bi-directional sharing of data, context and threat intelligence.

The typical SOC team has access to dozens of technologies, feeds and third-

THREATO'S NEWEST FEATURES INCLUDE A UNIQUE DATALINQ ENGINE FOR CONNECTING DISPARATE SYSTEMS AND SOURCES TO ENABLE EXTENDED DETECTION & RESPONSE (XDR), SMART COLLECTIONS FOR DRIVING AUTOMATION AND AN ENHANCED THREATQ DATA EXCHANGE...

party data sources. ThreatQ connects the dots, bringing this wealth of data together into a common work surface, providing datadriven security context that enables teams to be more thorough in their investigations, collaboration, response and reporting. The result is more efficient and effective operations that can be directly measured by time savings and FTEs gained, improved risk management, and greater confidence when detecting and responding LEON WARD

G

to an event.

"First generation SOAR, TIP and XDR technologies have helped SOCs wage their battle against evolving attacks, but not without limitations; it's time for security solutions to evolve as well. ThreatQuotient believes the foundation for the SOC of the future is data. which is why we doubled down on our DataLing Engine in v5 of the ThreatQ platform," said Leon Ward, VP of Product Management, ThreatQuotient, "Enabled by Smart Collections, organizations have a strong foundation today to get more out of their data. We look forward to releasing more market leading innovations in 2022, because all data is security data and needs to be incorporated effectively into the security lifecycle," he added.

ESET NAMED MAJOR PLAYER IN TWO MODERN ENDPOINT SECURITY IDC MARKETSCAPE REPORTS



in Modern Endpoint Security for Enterprise and SMB by the IDC MarketScape

ESET, a global leader in cybersecurity,

has been recognized as a Major Player in two IDC MarketScape reports – the Worldwide Modern Endpoint Security Enterprise 2021 Vendor Assessment (Doc #US48306021, November 2021), and the Worldwide Modern Endpoint Security SMB 2021 Vendor Assessment (Doc #US48304721, November 2021). Together, the reports assess vendors' endpoint security offerings across the SMB and enterprise markets.

Through a mix of surveys and interviews with market leaders, participants and end users, IDC MarketScape is known for providing in-depth quantitative and qualitative technology market assessments of different vendors' capabilities. The reports' assessment criteria focused on two main categories – an organization's capabilities and its strategies. While the capabilities category focuses on the company's offerings today, the strategies category looks at how the vendor's strategy will deliver on what customers need in three to five years' time.

The two reports focus on the importance of robust modern endpoint security for organizations both small and large. Modern endpoint security products protect personal computing devices from cyberattacks through detect and response mechanisms. One of the two mechanisms, endpoint protection platforms (EPP), reach detection verdicts and initiate responses in real time and autonomously, without human involvement. Endpoint detection and response (EDR) is the second stage of detection and response against cyberattacks that have evaded EPP detection. With EDR, the time to reach detection verdicts and initiate responses can span minutes to days depending on the severity of the threat itself.

YESWEHACK ESTABLISHES META PRESENCE, APPOINTS RABIH ACHKAR TO LEAD REGIONAL EXPANSION





YesWeHack, Europe's leading Bug

Bounty and Vulnerability Disclosure Policy (VDP) platform, has announced the appointment of Regional Director for the Middle East, Turkey, and Africa, Rabih Achkar, to spearhead the company's expansion in the region.

Rabih Achkar will be instrumental in supporting and advising organisations of all sizes and sectors on how they can successfully adopt a bug bounty model, RABIH ACHKAR WILL BE INSTRUMENTAL IN SUPPORTING & ADVISING ORGANIZATIONS OF ALL SIZES AND SECTORS ON HOW THEY CAN SUCCESSFULLY ADOPT A BUG BOUNTY MODEL AND THE IMPORTANCE OF A COMPLEMENTARY VULNERABILITY DISCLOSURE POLICY.

and the importance of a complementary Vulnerability Disclosure Policy.

RABIH ACHKAR

"We are here to offer to the region's digital ecosystem, a transformational approach to cyber audits through our crowdsourced security platform," said Rabih Achkar. "Governments across the region have worked long and hard to support their communities, foster innovation and drive sustainable growth. But their efforts are under threat from malicious parties who are continually evolving their techniques to evade cyber defences," he added.

TENABLE NAMED A LEADER IN INDUSTRIAL CONTROL SYSTEMS SECURITY BY INDEPENDENT RESEARCH FIRM

Tenable, Inc., the Cyber Exposure

company, has announced that it has been named a Leader in Forrester's report, "The Forrester Wave™: Industrial Control Systems (ICS) Security Solutions, Q4, 2021."

In its first-ever ICS Security Solutions Wave, Forrester evaluated vendors' capabilities across 27 different criteria and categorized them as Leaders, Strong Performers,

Contenders and Challengers. As one of only three leaders, Tenable received the highest possible scores (5.0) in seven criteria, including ICS Protocol Support, Vulnerability Risk Management for Operational Technology, Execution Roadmap, Innovation Roadmap, Planned Enhancements, Commercial Model and Product Security.

"Tenable.ot was superior to other vendors in this evaluation on the breadth of ICS protocols it can properly support..." according to Forrester's report. "Tenable. ot is a great fit for customers who already use Tenable in their IT environment for vulnerability risk management and

TENABLE.OT WAS SUPERIOR TO OTHER VENDORS IN THIS EVALUATION ON THE BREADTH OF ICS PROTOCOLS IT CAN PROPERLY SUPPORT, ACCORDING TO FORRESTER'S REPORT. seek to better understand the risks in their OT environment."

As escalating attacks on critical infrastructure continue, organizations struggle with gaining unified visibility across their dynamic environments of



legacy operational technology (OT), internet-connected ICS and modern IT. To address this challenge, Tenable. ot™ allows organizations to benefit from the efficiencies and cost savings of converged IT and OT environments in a risk-informed way. "The rush to modernize critical infrastructure and the ICS that underpins it has converged the worlds of IT and OT. It's no longer adequate to address the security of these environments in a siloed, disjointed fashion," said Nico Popp, chief product officer, Tenable. "Understanding exposure across the expanding ICS attack surface is the first and most important step in reducing overall risk. We're thrilled that Forrester has recognized us as a Leader with the highest possible scores in the execution roadmap and innovation roadmap criteria."

NICO POPP

NEW KASPERSKY ENDPOINT SECURITY CLOUD KEEPS SENSITIVE CLOUD DATA SAFE



The new version of Kaspersky

Endpoint Security Cloud now provides visibility and control over corporate files containing personally identifiable information (PII) or bank card details stored in Microsoft 365 applications. The product detects such files, so IT security managers can make sure that they are stored according to corporate policy and, more importantly, cannot be accessed from outside of the company.

Personally identifiable information still remains the type of data most commonly involved in breaches (43%), according to a Kaspersky study. Up to 15% of files stored in cloud services, such as SharePoint or Teams, which contain sensitive data, turn out to be shared with someone outside of the

company's staff circle. IT and IT security teams need to know if this risk arises to minimize the likelihood of this information getting into the wrong hands and ensure that the business follows data protection regulations.

The new Data Discovery capability in the updated Kaspersky Endpoint Security Cloud provides visibility over this cloud data. It gives IT managers a list of the files that are stored anywhere in Microsoft cloud applications – including SharePoint Online, OneDrive and Teams – and contain any item of PII or bank card data. This includes data such as

driving licenses, identity cards, passports, residence permits, social security, and taxpayer information. The product ensures 100% detection rate of PII regardless of the structure. delimiters they are written with and file extensions, as confirmed though a recent AV-TEST study using German data.

COHESITY GOES BEYOND ZERO TRUST WITH NEW SAAS SOLUTIONS DESIGNED TO ADDRESS INCREASINGLY SOPHISTICATED RANSOMWARE ATTACKS

COHESITY

To help customers address the latest threats, Cohesity has unveiled the following SaaS offerings -- which will be housed under the company's Data Management as a Service portfolio of Cohesity-managed solutions:

• Cohesity DataGovern: a data security and governance service that uses AI/ML to automate the discovery of sensitive data, and detect anomalous access and usage patterns which could indicate a cyberattack in play -- key to thwarting bad actors trying to exfiltrate data.

• Project Fort Knox: a service that will allow customers to maintain an isolated copy of their data in a Cohesity-managed vault to improve data resiliency in the face of ransomware attacks. In addition to immutability, this gives customers another way to thwart attackers trying to encrypt data.

These offerings will be key additions to the company's comprehensive Threat Defense architecture that showcases how

Cohesity, and a wide-range of ecosystem partners, help customers address the latest cyber threats, including ransomware.

"Cybercriminals are rapidly becoming more sophisticated and aggressive,

THESE OFFERINGS WILL BE KEY ADDITIONS TO THE COMPANY'S COMPREHENSIVE THREAT DEFENSE ARCHITECTURE THAT SHOWCASES HOW COHESITY AND ITS ECOSYSTEM PARTNERS HELP CUSTOMERS ADDRESS CYBERTHREATS.

THE NEW DATA

DISCOVERY

ΤΗΕ ΠΡΠΔΤΕΠ

KASPFRSKY

FNNPOINT

SECURITY CLOUD

PROVIDES

VISIBILITY OVFR

CLOUD DATA_

CAPARII IT

and the damage ransomware attacks cause to organizations can be catastrophic in terms of costs and brand reputation," said Matt Waxman, head of product, Cohesity. "Relying on legacy backup as an insurance policy no longer is sufficient. Customers need next-gen technology

that makes it easy to identify sensitive data, detect anomalies, isolate data, and stay ahead of modern threats. That's what we're focused on providing via our solutions and our Threat Defense architecture," he added.

FORTINET UNIFIES ZERO TRUST, ENDPOINT & NETWORK SECURITY TO LEAD WORK-FROM-ANYWHERE ERA

Fortinet, a global leader in

broad, integrated, and automated

cybersecurity solutions, has announced the industry's most complete solution to enable organizations to secure and connect work-from-anywhere. By unifying Fortinet's broad portfolio of zero trust, endpoint, and network security solutions within the Fortinet Security Fabric, Fortinet delivers security, services, and threat

intelligence that seamlessly follow users whether on the road, at home,

BY UNIFYING FORTINET'S BROAD PORTFOLIO OF ZERO TRUST, ENDPOINT & NETWORK SECURITY SOLUTIONS WITHIN THE FORTINET SECURITY FABRIC, FORTINET DELIVERS SECURITY SERVICES & THREAT INTELLIGENCE THAT SEAMLESSLY FOLLOW USERS. or in the office to provide enterprisegrade protection and productivity. These capabilities – designed for the way business is done in the Work-from-Anywhere Era – are available now.

John Maddison, EVP of Products and CMO at Fortinet, said: "Empowering users to move seamlessly between different work environments



has critical implications for maintaining user productivity as well as security. Cybercriminals have been quick to exploit the expanded attack surface and security gaps created by this shift in work patterns to get a foothold into the corporate network. Today's enterprise organizations require work-fromanywhere security that is as flexible and dynamic as today's business demands. Fortinet is the only vendor capable of delivering unified security built for the Work-from-Anywhere Era that seamlessly adapts based on a user's environment and risk profile."

QUALYS CLOUDVIEW ADDS SECURITY FOR INFRASTRUCTURE AS CODE ENABLING DEVSECOPS TEAMS TO START &STAY SECURE



Qualys, Inc, a pioneer and leading

provider of disruptive cloud-based IT, security and compliance solutions,

has announced it is adding Infrastructure as Code (IaC) scanning to its CloudView app. This will enable detection and remediation of misconfigurations early in the development cycle, removing risk in the production environment.

As noted in the (ISC)2 2021 Cloud Security Report, security professionals' biggest threat with public clouds is the misconfiguration of resources. Misconfigurations are often detected

LEVERAGING THE QUALYS CLOUD PLATFORM & ITS INTEGRATED APPS, CUSTOMERS CAN NOW INSERT SECURITY AUTOMATION INTO ALL STAGES OF THEIR APPLICATION LIFECYCLE, ENSURING COMPLETE VISIBILITY INTO BOTH RUNTIME AND BUILD-TIME POSTURE, VIA A UNIFIED DASHBOARD. post-deployment, leaving companies with a much larger attack surface and more vulnerable to exploits. Increasingly, organizations are using IaC to deploy cloud-native applications and provision their cloud infrastructure. Thus, it's important to shift security left to identify and remediate misconfigurations

SUMEDH THAKAR

JOHN MADDISON

at the IaC template stage. Detecting security issues earlier in the development cycle accelerates secure application delivery and fosters greater collaboration between DevOps and security teams. More importantly, it enforces better security policies in the production environment.

"With the addition of IaC assessment to CloudView, Qualys is extending its cloud security posture management (CSPM) solution to handle shift-left use cases," said Sumedh Thakar, president and CEO of Qualys.

"Leveraging the Qualys Cloud Platform and its integrated apps, customers can now insert security automation into all stages of their application lifecycle, ensuring complete visibility into both runtime and build-time posture via a unified dashboard," he added.

hat are some of the trends in the video surveillance market? There are some trends

that are dominating the video surveillance market such as video resolution. This has upgraded from standard resolution to higher resolution. Such as 4mp, 5 mp etc. Also, the system itself is upgraded from Analog to IP and this change is happening here in the UAE and countries in the Middle East. The application of AI in video surveillance is also a growing trend. Currently, most of HIKVISION's cameras as well as recorders have smart functions and AI-embedded features. Now, CCTV is also moving away from providing just security, to be used in day-to-day applications as well. Businesses are using CCTVs to add value.

Another trend in this area is called VSaaS or Video Security-as-a-Service. VSaaS is the technology that hosts the hardware and software of video-based security systems in the cloud, so that users can access their IP cameras anywhere through any device and have the video footage at their fingertips. Since there is no hassle of on-site server installation and system configuration, VSaaS is an ideal choice for small- and medium-sized businesses (SMB). It is more cost-effective than traditional video security solutions since users can spread costs out over the contract term and pay only for the services that are actually used.

> "MOST OF HIKVISION'S CCTV PRODUCTS HAVE BEEN UPGRADED TO BUILD-INTO ACUSENSE TECHNOLOGY. THIS DETECTS INTRUSION THREATS IN REAL TIME AND TRIGGERS ALERTS TO USERS' MOBILE PHONES FOR FASTER RESPONSE."

What are some of Hikvision's products and the key features of some of these products?

Most of Hikvision's CCTV products have been upgraded to build-into AcuSense technology. This detects intrusion threats in real time and triggers alerts to users' mobile phones for faster response. AcuSense intelligently identifies people and vehicles. AcuSense technology is combined with intrusion detection or line crossing which allows a user to define an area where a target should be identified. AcuSense technology uses advanced machine vision Al algorithms built into Hikvision security cameras and video recorders to boost home and business security. Hikvision AcuSense technology uses a filtering system to classify targets as humans, vehicles, or "Other" objects. With a powerful deeplearning algorithm at its core, it can intelligently differentiate between moving objects like shadows, leaves, animals, and other such unexpected movements.

Today's new technologies have also empowered modern video cameras to see better in any light and in high



resolution. Hikvision's security cameras with their signature ColorVu technology are great examples of this. These cameras guarantee video with vibrant colours even in extremely dark scenarios. A nextgeneration series of the cameras goes even further, using 4K Ultra high definition (UHD) to deliver crisp images that provide richer detail.

On the access control side, we're also upgrading our fingerprint devices to include facial recognition as well. Hikvision Access Controllers offer users various functions of access control. With its high adaptability, the device is suitable for a range of different application scenarios, and can be integrated with various other devices, such as card readers, locks or push buttons, to satisfy any user's unique requirements.

Access control systems serve a critical role in any sensitive area, allowing only

the right persons to enter at a given time. Multiple configurations cater to various budgets and needs, ranging from the simplest card reader to the now commonly used fingerprint terminals, to the algorithm-enabled facial recognition terminal. Hikvision's many devices – such as controllers, card readers, turnstiles, and door locks – offer you a complete and secure access control system.

As customer requirements grow more complex, a single solution can no longer fulfill every need. That is why you can combine our access control systems with various authentication methods such as ID cards, fingerprints, passwords, facial images, and QR codes, to name a few.

On top of basic functions, Hikvision hardware extends to advanced access management through anti-passback, combined authentications, interlocking, and more. And the professional management software makes device registration, management, and personnel registration much easier.

What are some of the products that are in high demand in the Middle East?

We have divided the market into four parts: Home users, SMB businesses, enterprise business and government businesses. For home end users, what is mostly in demand are hi-resolution videos and good after sales service. They also want their CCTV and other smart home devices to be linked, for easier use.

SMBs, on the other hand, are looking for reliable, cost-effective products. Enterprise clients look for integrated security features that are intuitive and easy to manage, while governments clients look for a centralised management platform of smart devices and so their demand for AI products is much higher.

AI IS A POWERFUL BROOM FOR CLEANING UP CLUTTERED SECURITY ENVIRONMENTS

ANOOP DAS, CYBERSECURITY EXPERT AT MIMECAST



Anoon Das

he stunning growth of the global cybercrime industry is putting strain on organisations and their security teams. Mimecast's latest State of

Email Security Report 2021 found that 45% of organisations in the UAE reported an increase in the sophistication of incoming cyberattacks, while 41% cited a growing volume of attacks. The increasing reliance on email and other business productivity tools is creating new challenges. In fact, three-quarters (75%) of organisations expect an email-borne attack will damage their business this year.

Security teams in turn look to deploy new tools and solutions to protect vulnerable users and systems, and this is warranted. The increase in brand impersonation attacks, for example, has made solutions such as DMARC and brand exploit protect tools invaluable to efforts to protect customers from compromise.

An lover abundance of security tools

However, the arowing number of security tools is also leading to cluttered security environments that can be hard to manage. One study puts the average number of security tools at any given enterprise at 45 others believe it's closer to 75.

What's interesting is that having more security tools does not necessarily equate to a better security posture. An IBM study found that enterprises using 50 or more security tools ranked themselves 8% lower in their threat detection capabilities and 7% lower in their defence capabilities than their less cluttered peers. The ongoing cybersecurity skills shortage presents a major challenge when it comes to managing security environments. Some analysts estimate that there is a global shortage of three million cybersecurity professionals, at a time when cyber threats have drastically increased in both volume and sophistication. Without the right personnel to manage the technology and ensure that everything is always properly enabled, having dozens of security solutions can cause more trouble than good. Which is why having too many security tools doesn't necessarily translate into better protection.

This may explain the growing adoption of artificial intelligence within security teams. The AI market for cybersecurity is expected to grow from \$8.8-billion in 2019 to more than \$38-billion by 2026, as the adoption of IoT and connected devices and a growing volume of cyberattacks put pressure on internal teams.

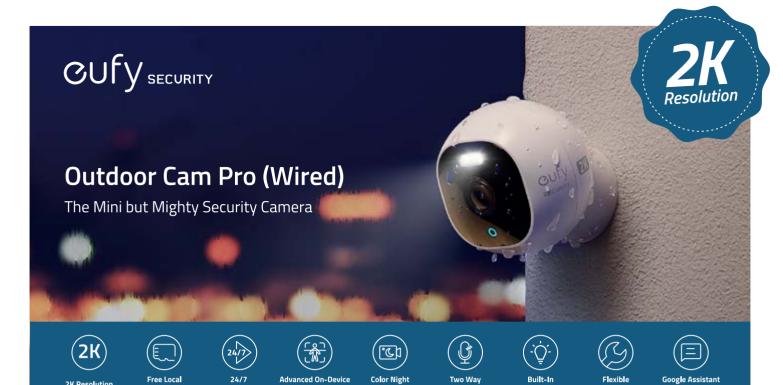
Decluttering security environments with AI

For most security professionals, security intelligence is still very much carbon based. not silicon based. In other words, for most security professionals, it's people and not tech that generate the highest-quality, actionable intelligence into security.

What do organisations need to bear in mind when determining what role AI could play in supporting security teams?

For one, AI is of little use when it is not integrated to the organisation's broader security ecosystem. Security teams should be able to integrate the findings of the Al tool into their other security tools to provide a unified and automated view of current and emerging threats. Having the AI tool assume some of the complexities of human behaviour also increases its usefulness. The sheer volume of data that most organisations have to manage also makes it near-impossible for security teams to remain effective without the assistance of algorithms. Setting clear expectations for what return-on-investment you seek for an Al deployment also makes positive outcomes more likely. Implementing an AI tool may require time and resources, which need to be factored in upfront.

Although it is no silver bullet, AI can be a powerful tool in helping organisations build greater resilience, and can lend welcome support to under-pressure security teams. However, it is essential that security leaders understand the role and limits of AI upfront, lest it becomes yet another solution cluttering up the security environment.





Storage

Recording

AI Detection

Stunning Colors and Detail

2K Resolution

ULTRA 2K resolution and the F2.0 aperture work in tandem to produce vivid images that give you the complete picture.



Vision

Audio

Spotlight

Secure in Extreme Weather Conditions

With an IP67 weatherproof-rating, Outdoor Cam Pro boasts greater protection against the elements than any of its competitors.



ind Alexa

Subscription Free Security

Installation

Equipped with a 32GB memory card and on-device AI, Outdoor Cam Pro offers security that is ready out of the box. *The device can support up to 128G.



Notifies You Only When Needed

The camera's built-in AI accurately identifies when a person is present. This means that you are only notified when an event occurs that requires your attention.



Color Detail at Night

The built-in spotlight illuminates the surrounding area when motion is detected and allows the camera to capture footage in vivid color. Giving you a much clearer view of who's there.



Flexible Installation

The Magnetic Mount and 20ft Cable allow you to easily install the camera anywhere on your property.

AED 299/-

CUL Innovations

Available at all leading electronics stores.

ENCHANCING CYBER DESELEMENTE RESILEMENTE METAMOLICAL METAMOLICAL ACCOR

JOHN DOLEY, REGIONAL SALES DIRECTOR - META WHO LEADS THE ACCESS MANAGEMENT SOLUTIONS AT THALES TELLS ANITA JOSEPH, EDITOR, SECURITY ADVISOR MIDDLE EAST, THAT IT IS IMPORTANT TO LOOK FOR A SOLUTION THAT CAN PROTECT AND INTEGRATE WITH ON PREMISES AND CLOUD SERVICES TO HELP REDUCE COMPLEXITY AND HELP WITH REGULATORY COMPLIANCE AT THE SAME TIME.



Cyber-attacks are on the rise and are becoming increasingly damaging. This is evident by the significant increase in ransomware attacks which are being carried out against all components of an organisation's infrastructure. According to Group IB, ransomware attacks grew by 150% during 2020.

What has 2020 taught you? What are the key learnings?

Cybersecurity professionals are always prepared to adapt. Our role is centered around helping businesses understand the potential risks and new threats and events that could put organizations' sensitive information, whether it is customer data or IP at risk. We have learned a great deal over the last year, but I would like to highlight three major learnings:

1. Cyber Resilience is an important business enabler in time of crisis. The pandemic has fast tracked the digital transformation journey and the urge to go remote instantly meant pushing forward with investment in cloud, connectivity, CYBER CRIMINALS CONTINUE TO SEARCH FOR EASY ACCESS AND WILL CONTINUE TO EXPLOIT GAPS LEFT BY WEAK AUTHENTICATION METHODS.

John Doley Thales Group automation, and innovation that could have taken longer time to deploy in normal times. As we adapted to these new technologies and digitalization we were exposed to new risk and challenges.

Even in the face of elevated threats, information security teams have risen to exceptional levels to support their organizations. But those organizations that were well equipped with an empowered and proactive security team could control and which were supported by robust processes and effective technology were in a better shape than the others.

2. Zero trust moves into the mainstream. The new wave of virtual workforces and the acceleration to adopting new technologies in a very short span of time gives us more reason to focus on security. With this in mind, making each device or user earn the trust to get on the network seems to be the way our security professionals are going to handle this escalation of connecting everything to the network. So our best bet is not to trust anything and move the risk/ trust down to a Zero Trust Network.

The maturity to Zero Trust Network will take time and effort. We have seen organizations incorporating Zero Trust functionality incrementally as part of a strategic plan which definitely reduces risk accordingly at each step. As the Zero Trust implementation matures over time, enhanced visibility and automated responses will allow our security professionals to keep pace with the threat.

A significant challenge to achieving Zero Trust is finding solutions that cover identities. Enforcing access decisions dynamically at the application access point, irrespective of where the user resides and the device they are using. So, we could say Zero Trust starts with Managing Access to the network. **3. Remote workforce challenges.** We see that security and risk management leaders are experiencing widespread disruption in Identity and Access Management space for many reasons, most notably because of the increased drive in user interactions on digital channels and the sudden and rapid expansion of the remote workforce because of the pandemic. The adoption of microservices architectures, move to the cloud, digitalization of modern world and increase in cybercrime incidents have made it more difficult to manage users.

Cyber criminals continue to search for easy access and will continue to exploit gaps left by weak authentication methods. Unfortunately, a 'one size fits all' approach to authentication is no longer feasible as users are expecting to be able to authenticate from anywhere and on any device.

As data breaches continue and compliance mandates get more stringent, how can organisations protect sensitive data in both onpremises and cloud environments? The first line of defence in protecting data in both on-premises and cloud environment is to make sure organizations have plugged in all gaps



in their authentication footprint with a solution that can offer policy based access allowing them to enforce to earn the user trust by a broad range of authentication methods.

It is important to look for a solution that can protect and integrate with

CYBERSECURITY PROFESSIONALS ARE ALWAYS PREPARED TO ADAPT. OUR ROLE IS CENTERED AROUND HELPING BUSINESSES UNDERSTAND THE POTENTIAL RISKS AND NEW THREATS AND EVENTS THAT COULD PUT ORGANIZATIONS' SENSITIVE INFORMATION, WHETHER IT IS CUSTOMER DATA OR IP AT RISK.



on premises and cloud services to help reduce complexity and help with regulatory compliance at the same time.

As cloud migration continues at a frenetic pace, tell us how Thales helps organisations in this journey.

It is important that your organization strive to find a suitable balance between user experience and security especially in the context of today's remote and/or hybrid workforces, cloud transformation and enterprise apps. Modern authentication comprises the latest innovations in authentication technology, which have been developed to enable authentication in a cloud based world. Thales can help organizations by:

• Protecting on premises and cloud services and apps

• Offering a powerful range of authentication methods that can support multiple authentication journeys • Easily and flexibly integrating into an IT environment

What, in your opinion, are some of the best practices for secure cloud migration? What are organisations missing/overlooking?

Prepare for the threat: Create, maintain, and test encrypted, offline backups of critical data. Develop and exercise both a cyber incident response & communications plan. Make digital asset management a key competency for your organization. Create and maintain a cybersecurity awareness training program for your users.

Centralize Identity Management: In a hybrid identity scenario, organizations must integrate their on-premises and cloud directories. With this integration, the security teams can manage accounts from one location, irrespective of where the account is created. It also enables users to access both cloud and on-premises resources with a common identity.

Make sure secure access and identity protection is at the heart of your security strategy – identity is the new security perimeter. Don't leave any authentication gaps, ensure you select a service that is scalable and flexible that can grow with your needs. Here are a few best practices to consider specific to authentication:

Adopting MFA and modern authentication for Critical Apps -Critical apps that provide key services to employees or that give access to your network should be protected by a modern authentication solution that is able to make intelligent access decisions and enforce the right level of authentication. These critical apps differ across organizations, but they typically include VPN, remote desktop, cloud computing platforms, and customerfacing applications.

Carefully Consider Authentication Factors - The choice of authentication factors is where user experience comes into the equation. Whether your users are employees or customers, you don't want to alienate them by making it frustrating to log in to your app or to perform specific actions within your applications. For customer-facing authentication, a prudent strategy is to utilize adaptive authentication and combine it with other methods of stronger authentication when needed. The key here is to offer users a range of authentication options, such as a FIDO security keys, OTP tokens, or push notification on their registered smartphone.

Monitor Identities Actively – Monitoring identities actively can help organizations quickly detect suspicious activities and trigger an alert to prevent the threat. You can be at risk of user credentials being compromised failing to do so.

TIMELY ACTION TO PREVENT CYBERATTACKS

KARIM ABILLAMA, PRE- SALES DIRECTOR, INTERNATIONAL BUSINESS. NETWITNESS HAS A CHAT WITH NITYA RAVI ABOUT THE CURRENT CYBERSECURITY I ANDSCAPE IN THE REGION.



hat is vour take on the current cybersecurity scenario and how does the NetWitness offer fit into the same?

The pandemic has created a new world where everyone is working from not just one location but from wherever they prefer. Everything is remote, even security operations. Even security operation teams and analysts are operating and collaborating remotely. That obviously expands the potential points of attack on enterprise networks.

Prior to the pandemic and even now, we are finding large enterprises enabling remote access to their entire work force. whereas before they may have only allowed remote work to a small percentage of their workforce. The result of this trend is that the threat landscape is larger and enterprises are at a higher risk of cyber-attacks.

Cybersecurity is evolving and pushing enterprises to place increased focus on their cybersecurity postures. They now



require the ability to monitor and analyse what is happening in their network, and whether an outside threat actor is trying to access their systems. These organisations must employ the right measures and monitoring tools in place to detect threats and respond immediately.

The NetWitness Platform provides enterprises with the visibility needed to detect sophisticated threats across all capture points – including logs, packets, netflow, endpoint and IoT – and physical, virtual and cloud computing platforms, and take quick action to investigate, analyse and mitigate those threats.

How is NetWitness helping larger organisations to move forward in their digital transformation process, in safety?

Many larger organisations with critical infrastructures, like defense organisations, already have a security operations centre (SOC) in place. For these organisations, they turn to us for help for a robust platform that detects threats quickly. We reduce the time to detect the threat and investigate it. Security analysts traditionally suffer from alert fatigue – after all, they are being inundated with information and notifications about potential security "PRIOR TO THE PANDEMIC AND EVEN NOW, WE ARE FINDING LARGE ENTERPRISES ENABLING REMOTE ACCESS TO THEIR ENTIRE WORK FORCE, WHEREAS BEFORE THEY MAY HAVE ONLY ALLOWED REMOTE WORK TO A SMALL PERCENTAGE OF THEIR WORKFORCE."

issues. The NetWitness Platform helps organisations make sense of all that data and then take timely action. Our tools help to prioritise threats that matter most to the organisation, and which can cause damage to the business. Even companies without a SOC can use the NetWitness Platform, as well as some of our professional services, to protect their infrastructures.

What is your opinion about the security landscape in the UAE and the mindset towards adoption of new technology?

The UAE is one of the world's fastest-paced technology adopters. The government here is currently encouraging digital transformation, and that is wonderful. That focus makes this region unique and means that technology adoption is much quicker here than in other parts of the world.

In the GCC, the UAE and Saudi Arabia is at the forefront of technology adoption. The willingness of enterprises to adopt different technologies in their business plans also means there is an increased need for visibility into their critical systems. The challenges that enterprises face with digital transformation here are similar to the ones faced by other companies undergoing rapid change: they need to ensure that no matter what technologies are implemented, no matter where their employees are based, no matter how they are serving their customers, they are doing so from a position of cybersecurity readiness. **1**



YOUR DATA IS YOUR BUSINESS



ENDPOINT

SECURITY



DATA ENCRYPTION



SECURE

AUTHENTICATION





DETECTION &

RESPONSE





CLOUD

SANDBOXING



MAIL SECURITY

MAKE SURE YOUR COMPANY IS SAFE FROM DATA BREACHES OR LEAKS. EMPLOY OUR POWERFUL AND EASY TO DEPLOY ESET SECURITY SOLUTIONS.



400k+

business customers

200+ countries & territories **13** global R&D centers

WWW.ESET.COM/ME

ISSUE 60 | NOVEMBER 2021

WWW.TAHAWULTECH.COM



SPECIAL REPORT SECLORE: SECURITYNOW

SECURITYNOW: SECLORE'S FLAGSHIP EVENT FOR KEY INSIGHTS ON DATA SECURITY

THIS YEAR, THE EVENT FACILITATED CRUCIAL DISCUSSIONS ON THE CHANGING DATA SECURITY LANDSCAPE AND BROUGHT TOGETHER SOME OF THE BEST MINDS IN THE FIELD FOR INSIGHTFUL DEBATES AND KEY LEARNINGS.



eclore's much-anticipated annual flagship event, SecurityNow, brings together experts in security and technology to discuss

and explore the data security landscape, challenges, ways to address them and chart the way ahead. This year-the fifth consecutive year of hosting this event and the second year of doing so virtually-brought together experts and a stellar line-up of speakers to focus on the topic of Secure 3rd Party Collaboration... Cloud & Beyond.

The event, which took place on October 6 and 7, was hosted on the BrightTALK platform and included panel discussions, keynote speeches, customer stories, tips, insights and an engaging fireside chat with Hamed Shahbar, VP & Head of Network and IT, Public Investment Fund (PIF). THE EVENT, WHICH TOOK PLACE ON OCTOBER 6 AND 7, WAS HOSTED ON THE BRIGHTTALK PLATFORM AND INCLUDED PANEL DISCUSSIONS, KEYNOTE SPEECHES, CUSTOMER STORIES, TIPS AND INSIGHTS ON THE CHANGING DATA SECURITY LANDSCAPE.

Vishal Gupta, CEO of Seclore, opened the event with a welcome note, highlighting the need for secure external collaboration.

"Enterprises are most worried about confidential information they have to send to external agencies such as partners, vendors, contractors, lawyers, etc., and hundreds of other companies surrounding the enterprise," he said.

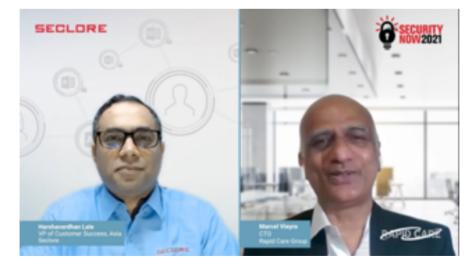
Todd Fennell, VP of Information Security, American Express, delivered the keynote address about how secure collaboration, privacy regulations, and the Zero Trust framework affect the information security landscape of the banking industry.

"Most people like to say that the perimeter is dead or is not as effective as before. But I would submit that perimeter is still highly effective. The challenge comes with clearly defining what lies within the perimeter and what does not. The perimeter sometimes changes on a day-to-day basis depending on the business processes used," he said.

The keynote address was followed by a product roadmap session conducted by Abhijit Tannu, CTO of Seclore and Zubin Dalal, Sr Director of Product Management at Seclore Technology, who spoke about Seclore's future plans and growth trajectory. This was followed by an engaging hour of customer exchange sessions, where Seclore's customers shared their experience of how Seclore was helping them in their journey towards data-centric security. This

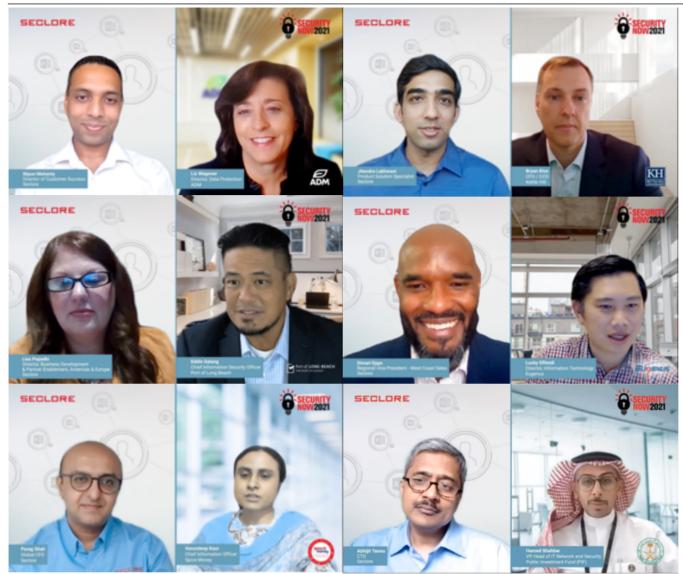






included the following testimonies: "Seclore's automated data protection has helped us build a data protection strategy during COVID times without hiring employees to monitor employees." - Marcel Vieyra, CTO, RapidCare Group

SPECIAL REPORT / SECLORE



"There are always going to be employees or external parties who will misuse the data intentionally or unintentionally. We need a solution that will allow us to stay at the top of the game." – Liz Wagoner

"To incorporate a data-centric security solution, it is necessary to first understand the data and its behavior. Adopting a solution without doing so may either prove to be overkill or just not enough." - Edward Galang, CISO, Port of Long Beach

"[Data] Security cannot be a tick-mark activity. We need a solution that will protect the information shared with third parties."-Varundeep Kaur, CIO, Spice Money.

"The best thing about using Seclore is I can sleep better knowing that my documents are safe, no matter where they are."- Bryan Kiss, CCO/CFO, Kettle Hill Capital Management.

"Seclore is the only solution that offers holistic data-centric security. It is the only solution that provides data security on the cloud, especially when using SharePoint day in and day out." - Lucky Effendi, Director of Information Technology, Eugenus, Inc.

Vishal Gupta, Seclore's CEO, Manjul Kubde, Chief Product Architect and Abhijit Tannu, CTO, then came together to highlight and respond to questions about the company's culture and talent acquisition process and outline its history and growth over the last few years.

Day 1 of the event closed with a series of product demos featuring some of Seclore's latest data-centric capabilities.

Day 2 opened with a welcome note by Manjul Kubde.

Viewers received the exclusive opportunity to be part of a stimulating panel discussion with Rob Oden of L3Harris Technologies, Monil Naicker of Applied Materials, and Evgeniy Kharam of Herjavec Group, moderated by Vishal Gauri from Seclore. They discussed how regulated industries manage the "mutually conflicting" goals of secure external collaboration and privacy compliance.

This was followed by a fireside chat between Hamed Shahbar, VP and Head (Network and IT) of Public Investment Fund, and Abhijit Tannu, CTO of Seclore. The discussion was centered around managing data security for one of the world's leading



MOST PEOPLE LIKE TO SAY THAT THE PERIMETER IS DEAD OR IS NOT AS EFFECTIVE AS BEFORE. BUT I WOULD SUBMIT THAT PERIMETER IS STILL HIGHLY EFFECTIVE.

sovereign wealth funds. They discussed how important it was to have data-centric security for such huge organizations.

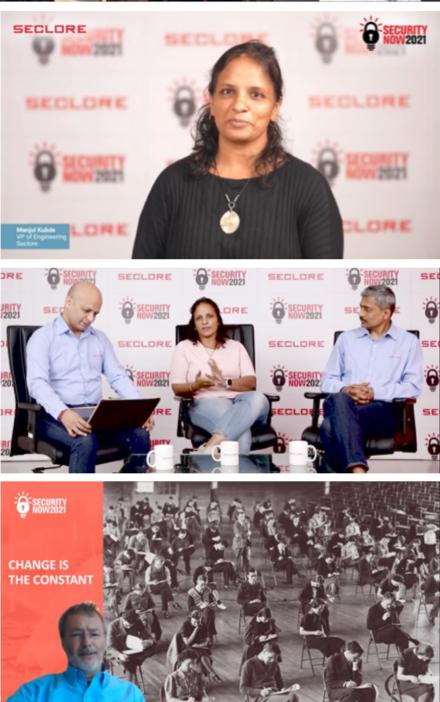
A second panel discussion was then conducted, with renowned security entrepreneurs-Arti Arora Raman of Titaniam, Kevin Coppins of Spirion, and Jim Barkdoll of Axiomatics. This session focused on how security could no longer afford to stay confined within the infrastructural limits and needed to move towards the critical asset we are protecting – data.

The event came to a close with a brief address by Jasbir Singh, Managing Director (Europe), of Seclore.

To sum up, SecurityNow 2021 provided the perfect opportunity for insightful discussions on how data-centric security can ensure secure external collaboration and how enterprises must shift their focus to data-centric security. The event also allowed attendees to see for themselves how two of the largest organizations in the BFSI sector manage data security and external collaboration.

Recordings of the event will soon be made available, along with other exciting eventrelated content.

Meanwhile, do visit our website www. seclore.com and follow our LinkedIn page for regular updates.



NEW-AGE DATA BACKUP& BACKUP& BACKUP& BASTORATION SHALVE VE METALLIC EMEA AT COMMVALUE TELLS ANITA JOSEPH A

SHAI NUNI, VP, METALLIC EMEA AT COMMVAULT, TELLS ANITA JOSEPH ABOUT METALLIC, A SERVICE THAT LETS ONE BACK-UP AND RESTORE DATA WITHOUT HAVING TO INSTALL AND MAINTAIN TRADITIONAL BACKUP SOFTWARE.





hat is your opinion about the ransomware scenario and the solutions we have

This is exactly the question that CIOs and CISOs are asking themselves. According to IDC and other analysts, ransomware attacks increased dramatically between 2019 and 2020 and this is expected to grow. The estimation is that ransomware attacks happen every 11 seconds around the globe. Those kinds of cyber-attacks have been there before COVID, but now, post the pandemic, most cybercriminals are capitalizing on the fact that people are working from home, so instead they look for holes in the network, ultimately leading them towards data centres. Before COVID, when we spoke of ransomware, customers said they didn't want to move their data to the cloud because of the imposing cyber threat, thinking that the cloud will expose them to ransomware attacks. They feared they wouldn't be secure



enough, as the data is public. But postpandemic, rampant ransomware attacks dramatically changed the behaviour of CIOs and CISOs, forcing them to think differently in order to protect businesses most critical asset – their data. They understand that even if they rely on external sources, they have to eventually take responsibility for protecting their data against whatever happens.

What about Metallic's solutions and how is the market responding?

Metallic, our award-winning Softwareas-a-Service solution, was a great idea that our CEO Sanjay Mirchandani brought to the table and grew to the industry differentiator it is today since its incubation in 2019. For us, the understanding that Commvault which was and still is, leading in the Gartner Quadrant in the data protection space for enterprises for nine years already, an industry leader, we anticipated the shift to the cloud will increase and accelerate even before the pandemic. He also realized that instead of acquiring METALLIC IS AN INTEGRATED CLOUD STORAGE TARGET THAT MAKES IT SIMPLE FOR IT ORGANIZATIONS TO ADOPT CLOUD STORAGE FOR COMMVAULT BACKUP & RECOVERY OR HYPERSCALE X – TO EASE DIGITAL TRANSFORMATION, SAVE COSTS, REDUCE RISK AND SCALE LIMITLESSLY.

another company for cloud protection, we already had the foundation of Commvault, built on 25 years of engineering and industry excellence, so why not use this to our advantage. While there are many competitors thinking similarly, they have siloes of solutions for the data centre, so he suggested to come out with Metallic, which will be data protection for the cloud for customers.

For Commvault, we knew that customers would shift more and more workloads into the cloud, so incubating a SaaS solution, birthed from our own solutions, was a no brainer. Today, we have an engineering of Metallic that co-operates with the engineering of Commvault, to use the power of Commvault and what we are, in fact, developing in the cloud. We call it the power of AND - the power and cohesion of Commvault and Metallic, will really give the customers the ability to be successful in their journey to the cloud.

In short, Metallic is an integrated cloud storage target that makes it simple for IT organizations to adopt cloud storage for Commvault Backup & Recovery or HyperScale X – to ease digital transformation, save costs, reduce risk and scale limitlessly.

PREVENTION FIRST

KEIRON HOLYOME, VICE PRESIDENT – UKI, MIDDLE EAST AND AFRICA, ON THE CHANGING CYBERSECURITY LANDSCAPE AND HOW BLACKBERRY'S STRATEGY OF PREVENTING PRE-EXECUTION MALWARE HELPS ORGANIZATIONS IN THE REGION GROW THEIR BUSINESS IN A SAFE AND SECURE MANNER.

hat challenges do you think organizations are facing today with regard to an overall cybersecurity strategy, especially post the pandemic?

I think I think pre-and post-pandemic, organizations struggle with the same thing- resources. Retaining and hiring resources in cybersecurity is really tough. It's also really expensive. Making sure you've got the right skills in place to cope with today's challenges is a really, really important thing, but the fact is, there simply aren't enough resources. As we gradually emerge out of COVID, I think that understanding where the workforce is going will be critical. But I think we'll continue to face the same challenges that there aren't enough people in cybersecurity and the processes and therefore, the products that we have, need to help with the issue.

There is a huge skill shortage in the cybersecurity market. So, what are your thoughts on what organizations need to do to prevent malware& ransomware, especially with shortage of so many skills?

Great question, and it goes straight to the heart of the Blackberry strategy, really. We love EDR-XDR and we think it plays an absolutely key part in "a" strategy, but it is not "the" strategy. Our view is that

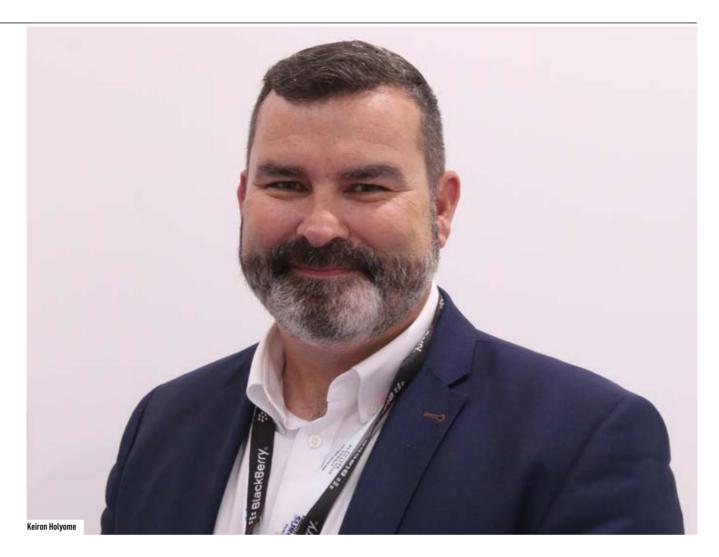
> OUR VIEW IS THAT PREVENTION FIRST IS THE STRATEGY SO, WHAT WE TRY AND DO IS ENSURE THAT OUR PRODUCTS HAVE A PREVENTION-FIRST CAPABILITY.

prevention first is the strategy so, what we try and do is ensure that our products have a prevention-first capability. What I mean by that is we prevent pre-execution malware happening in your environment in the first place. This does two things: one, it saves your organization's time and money because you are not chasing and threat hunting in the environment. Secondly, you can take the resources that you would be spending on that, whether it be money or individuals, and deploy them to the areas of your business which is, effectively, growing your business and other things that support that growth. So prevention first can be done, prevention is possible and BlackBerry's technology enables organizations to do that.

What can resellers/the channel ecosystem actually do to make sure that their products are secure and how can they help organizations stay secure in today's world?

We operate on the channel model, so we engage with our partners and our resellers, but no one organization can solve this challenge-we need to work collaboratively to make sure that we do two things: first, educate our customers. We're front and centre with our customers, educating the board that cybersecurity is now an issue, and boards are recognizing it's an issue. They recognize they must have the right people and the right skills and go and make sure that the brand and the reputation are safe.

Second: educating the users, making sure that users are getting the right input as to what they should be doing to protect themselves and the organization, and our partners play a key part in that. We are able to go and talk to many customers about the services we do, but we find that partners tend to have more resources and so are able to go talk to individuals and



organizations, probably about a broader set of technologies. So our partners are key, what we want from our partners is that they come and work with us, work with our customers. And as part of the overall cybersecurity landscape, bring solutions.

What has Blackberry been doing in the region and how has the company been keeping up with the changing technology and security scenario?

The region itself is undergoing massive change-in fact, change is a constant in the Middle East and we love that. Change, however, comes with risks, and the risks that we see are that this constant digitalization of our daily lives creates threat vectors for cybersecurity bad actors to get into our lives and our businesses. What Blackberry's doing specifically in this region, is that we're investing heavily into this region. So, we're bringing new teams

into the region- in fact we just hired some people in Saudi Arabia we're hiring people in Egypt, so we're bringing our skills and technology into the region, so that we can sit in the region with presence, and understand the challenges that the region has. We're also making sure that we have the programs in place to do the things I just talked about- basically making sure we're educating the partners- not in a way that we don't believe they've got the skill set, but by constantly updating them with the things that we're seeing in the market, specifically within the Middle East, specifically with the threat actors we're seeing in the Middle East, so that they can talk to their customers about making sure their environments are secure. So we continue to invest here, we think the Middle East is a fantastic growth area for Blackberry and our technology lends itself to that area.

What are some of the trends you think will drive the cybersecurity industry going forward?

The question goes back to where people are going to be working from, and there's no one answer. I think that a hybrid approach to where people are working is going to be the one that prevails, not just in this region, but in the rest of the world, and that challenges about how we deal with remote working securely will continue to be a challenge. But I also think that, as we come out of the COVID lockdowns and whatever we're going through now, things haven't changed much in cybersecurity. I think that we're still seeing many malware attacks and over 400,000 different types of malware every single day. So those challenges will persist, and we need to have the right technology, people and processes in place to deal with it. 1

ONLY THREE-FIFTHS OF MIDDLE EAST IT LEADERS FEEL CONFIDENT IN THEIR ABILITY TO RESPOND TO A CYBER INCIDENT TODAY

NEW RESEARCH FROM RACKSPACE TECHNOLOGY DELVES INTO THE STATE OF MIDDLE EAST BUSINESSES' CYBERSECURITY STRATEGIES.

nly 48% of organizations feel confident in their understanding of the cybersecurity threat landscape for their business, according to new research from Rackspace Technology. In addition, only three in five (59%) Middle East businesses feel confident in their ability to respond to incidents today.

A look into the Middle East business cybersecurity landscape

Constantly evolving security threats and attack methods, as well as increasing

"GIVEN THE CURRENT DIGITAL SKILLS GAP AND ONGOING RECRUITMENT CHALLENGES, IT IS IMPORTANT THAT BUSINESSES SEEK FURTHER SUPPORT FROM THIRD-PARTY PARTNERS TO HELP IDENTIFY AND ADDRESS THEIR WEAKNESSES." attack opportunities as data volumes, digital operations and remote work continue to grow, are cited by more than half (55%) of the Middle East's IT leaders as the greatest cybersecurity challenges their organization is currently facing.

In the face of this threat landscape, further concern is raised by the finding that nearly half (44%) of IT decision makers don't have the capability today to identify security incidents across multicloud environments. When it comes to mitigating threats, only 49% of those surveyed feel confident in addressing them today, and only half feel assured in addressing regulatory compliance.

In relation to data, about half (56%) are currently confident in their ability to protect critical data and warehouses. And when it comes to assessing cybersecurity capabilities and needs on a periodic basis, only two in five (45%) felt comfortable in this area.

The talent and skills gaps

Contributing to or explaining some of the ongoing challenges, more than half (64%) of companies are finding it hard to retain and recruit cybersecurity talent, though a similar proportion (61%) are confident in their internal initiatives in terms of cybersecurity talent retention.

The cybersecurity skills touted as the most important were cloud security (52%)

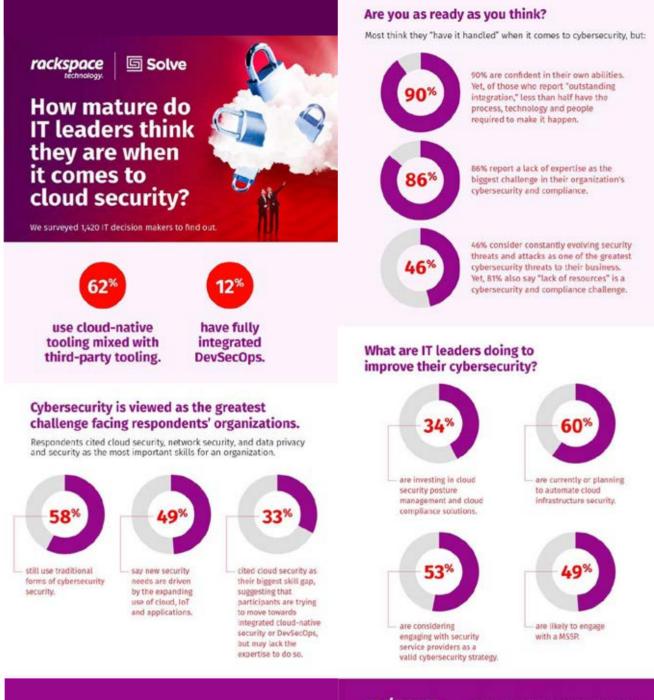
and risk management (50%). Despite its importance, a third (37%) of companies feel the biggest cybersecurity skills gap is in relation to cloud security.

Addressing the cybersecurity gaps with third-party providers

In the face of staffing and skills concerns, more than half of Middle East businesses (62%) rely on in-house staff with some external third-party help. A third (34%) said they use at least six to ten external partners to provide cybersecurity. When looking into the types of cybersecurity partner the businesses engage with, the most sought-after are Managed Security Service Providers (MSSPs) (48%) and System Integrators (45%). The top three areas of cybersecurity most likely to be handled by external partners are around integrated risk (52%), network security (45%) and data security (41%).

When asked to report their companies' overall level of maturity in cloud security, 34% said they were at intermediate level, having to rely on third-party tools built for cloud security. An additional 27% described themselves as cloud-centric, meaning they use native tooling mixed with third-party tooling.

George Pawlyszyn, Middle East and Africa General Manager at Rackspace Technology, said: "Cybersecurity is one of



rackspace

If shift intempolation, we, i Rampinian, Sandora Support, resultat Operanical' and Inter-Rampion multiplies of the service match or registered services and inflating-operation. In The Institute Installand other sections and other sections and installant match match installant sections.

the most important digital elements for Middle Eastern businesses, but also the trickiest to address. This is particularly true due to the accelerated pace of digital transformation across key sectors. Given the current digital skills gap and ongoing recruitment challenges, it is important that businesses seek further support from third-party partners to help identify and address their weaknesses.

"Factors such as the evolving threat landscape, remote working conditions and talent shortages all feed into the varying security needs from one business to the next. What is increasingly clear is that few businesses have all bases covered – people, processes and technology in place – when it comes to a mature cybersecurity model. Working with a partner that can bring these specialist skills and tailor them to specific requirements is an increasingly popular and effective way to ensure and increase overall confidence in addressing cybersecurity needs."

VIRSEC STRENGTHENS EXECUTIVE TEAM WITH KEY APPOINTMENTS

EXPANDED LEADERSHIP TEAM FURTHER POSITIONS COMPANY FOR HYPER-GROWTH AS MORE CUSTOMERS LOOK TO VIRSEC TO PROTECT THEIR SOFTWARE WORKLOADS AT RUNTIME





irsec, the only cybersecurity company to fully protect software at the workload while it is running, has announced executive appointments to

help lead the company through its next growth phase.

• Emmi Nguy, Vice President of Finance & Operations

• Marcelo Oliveira. Vice President of Product Management

•Thomas Schaeffer, Vice President of People

"We are on a mission to make cyberattacks irrelevant. Our ability to map what our customers' software is supposed to do and stop it from doing what it is not, due to ransomware attacks or other anomalies, is unrivaled," said Dave Furneaux, Chief



Marcelo Oliveira

Executive Officer of Virsec. "Our mission combined with our innovative technology is attracting the top talents in the industry to Virsec. These experienced executives are very highly regarded in their areas of practice and will play a pivotal role in our success as we embark on our hyper-growth journey as a company."

Emmi Nguy, Vice President of Finance & Operations

Nguy has more than 20 years of experience leading all aspects of financial governance and financial operations. Prior to joining Virsec, she served as VP of Finance, Strategy and Planning at Vectra AI, where she was instrumental in growing and scaling the company to \$1B+ in valuation.

Before Vectra AI, she held various finance management positions at global companies, including Juniper Networks and Johnson & Johnson.

Marcelo Oliveira. Vice President of Product Management

Oliveira is an industry veteran with over 20 years of experience in product management, product marketing, business development, and engineering. Oliveira has been working as a product management executive for over a decade across Cisco, Symantec, and, most recently, Contrast Security.

Thomas Schaeffer, Vice President of People

Schaeffer has several decades of experience leading People Operations, helping scale six technology companies from startup through IPO and beyond. Several of these IPO technology companies included Synopsys, StrataCom/Cisco, Juniper Networks, and, most recently, NIO.

With more than 50 patents, Virsec is trusted by Global 1000, midmarket, and public sector customers to protect their software workload at runtime. Its uniquely deterministic approach to security has earned many accolades, including a recent finalist nod for the prestigious ARN Innovation Awards 2021 and a win for the Best Emerging Security Vendor at the CISO50 & Future of Security Awards. 1

Russia has a powerful cybersecurity industry. We are No.1 in strong authentication, electronic signature and software protection domains.

Create a secure cryptographic environment at the state level for the exchange of essential information.



Strong authentication and electronic signature



Software monetization and protection against reverse-engineering



Consulting and training in cybersecurity

Be sure you are protected

Technologies for a secure future



aktiv-company.com

global.guardant.com



THE HUNT FOR CYBERATTACKS

MARTIN SUTHERLAND, GENERAL MANAGER, NETWITNESS, ON THE NEED FOR FORESIGHT ABOUT POTENTIAL SECURITY BREACHES.



Martin Sutherland



hat according to you are the main security challenges that the META organisations need to address?

There are some distinct security challenges faced by customers in the Middle East and Africa. Ransomware attacks are at the top of that list. There are ongoing and continuous attacks in the region. Around 42 percent of local business in the UAE that we survey says that there has been some level sort of business closure or shut down due to ransomware.

Ransomware is a major issue, however, it's not the ONLY issue. With the onset of the pandemic, a lot of organisations have undergone digital transformations that have enabled remote workforces, which rely on more digital tools and cloud resources. Many of these tools pose their own security risks. Most of the people assume that the cloud is secure but that is not necessarily the case. Organisations need to perform extra due diligence to ensure that they have the same level of security in the cloud as they would on-premise.

How does NetWitness help tackle this current increase of ransomware attacks? A lot of people believe that ransomware is



an attack where data is encrypted, and you pay a fee to fix it. While that's essentially true, it's more nuanced than that. The first incident is the attack or breach, but threat actors are in the system, what follows is a period when the encryption process occurs. This encryption process could take weeks to spread within the network, moving from one critical system to the next. That's why it's important to quickly detect these types of threats. For NetWitness, our mantra is detect, investigate and respond. Early detection of threats can help save some of the data in your network and mitigate the impact on the organisation.

Can you throw further light on this

On average, customers who pay the ransom are able to recover only 65% of their data. From those who pay the ransom, 25% could only decrypt less than a third of their data and 33% could only decrypt less than 50% of their data. Furthermore, about 80 percent of the people attacked by ransomware will get attacked again since the attacker might keep a "backdoor" in place to attack again later. Hence its quite important to address this quickly.

We have an Incidence Response team that helps companies investigate attacks onsite or remotely and uses our solutions "A LOT OF PEOPLE BELIEVE THAT RANSOMWARE IS AN ATTACK WHERE DATA IS ENCRYPTED, AND YOU PAY A FEE TO FIX IT. WHILE THAT'S ESSENTIALLY TRUE, IT'S MORE NUANCED THAN THAT."

to respond and hopefully prevent major impact. We not only investigate where the breach is but we move through the system laterally – just as an attacker would – which allows us to detect where the point of attack is and from where its spreading to other capture points. Our Incident Response team also checks for those "backdoors" that attackers like to leave, and remove them.

Why NetWitness and what are your key differentiators?

Cyberattacks are increasing both in frequency and sophistication. That means that security

teams need increased levels of visibility across their systems. The NetWitness Platform is a SIEM and XDR platform that accelerates threat detection and response. It can collect and analyse data across all capture points (logs, packets, netflow, endpoint and IoT) and computing platforms (physical, virtual and cloud), enriching data with threat intelligence and business context.

We also have a number of professional services offerings, including a global incident response team that trained to the highest level to hunt attacks. They come quickly and, in some places, also deploy our technology.

What is your take on the security landscape in the region and openness of the organisation in adopting new strategies?

I oversee a mix of mature markets like the UAE and less mature markets like in some parts of Africa. One of the things we focus on as a team is not to simply sell a technology but rather be a consultant to help customers. We come in and review the entire infrastructure and make recommendations about not just the technology, but also how to improve or automate processes, educate analysts and provide peace of mind to executives. Our aim is to be a trusted advisor in the region. **1**

FOCUS / MANDIANT

FIN12: THE PROLIFIC RANSOMWARE INTRUSION THREAT ACTOR THAT HAS AGGRESSIVELY PURSUED HEALTHCARE TARGETS

Kimberly Goody, Director of Financial Crime Analysis at Mandiant

andiant has released a comprehensive report detailing FIN12, an aggressive, financially motivated threat group

behind prolific ransomware attacks since October 2018. Almost 20% of the ransomware intrusions Mandiant has responded to in the past year were attributed to FIN12.

FIN12 is unique among many tracked ransomware-focused actors today because they do not typically engage in multi-faceted extortion and have disproportionately impacted the healthcare sector. They are also the first group promoted by Mandiant to a named FIN (or financially motivated) threat group who specialises in a specific phase of the attack lifecycle—ransomware deployment—while relying on other threat actors for gaining initial access to victims. This specialisation reflects the current ransomware ecosystem, which is comprised of various loosely affiliated actors partnering together, but not exclusively with one another.

According to Kimberly Goody, Director of Financial Crime Analysis at Mandiant, "FIN12 is one of the most aggressive ransomware threat actors tracked by Mandiant. Unlike other actors who are branching out into other forms of extortion, this group remains focused purely on ransomware, moving faster than its peers and hitting big targets. They are behind several attacks on the healthcare system and they focus heavily on high-revenue victims. Nothing is sacred with these actors – they will go after hospitals/ healthcare facilities, utilities, critical infrastructure, etc. This illustrates that they choose not to abide by the norms."

FIN12 victim organisations have been overwhelmingly located in North America; however, there is some evidence that FIN12's regional targeting has been expanding. Since the first half of 2021, they have targeted twice as many organizations outside North America. These organizations have been based in several countries, including the United Arab Emirates.

The group's targeting appears to be relatively industry agnostic but the group has disproportionately impacted healthcare organisations even in the midst of the COVID-19 pandemic. Almost 20 percent of observed victims have been in the healthcare industry and many of these organisations operate healthcare facilities. The remaining victims have operated in a broad range of sectors, including but not limited to business services, education, financial, government, manufacturing, retail, and technology.

The average annual revenue of observed FIN12 victim organisations was more than \$6 billion USD and almost all the organisations made more than \$300 million USD, based on data compiled from ZoomInfo.

Throughout FIN12's lifespan, the group has

relied upon multiple different threat clusters for malware distribution and the initial compromise stage of their operations. FIN12 has likely established close partnerships with these initial access providers; in most incidents where the initial intrusion was identified, FIN12 activity was observed on the same day as the initial access campaign.

Despite clear patterns across their intrusions, FIN12's post-compromise TTPs have evolved over time. This type of slow evolution is to be expected of any threat group that maintains operational coherence during a period of months or years. Some of the most important developments in FIN12's post-compromise TTPs have included changes in the way they've relied on TRICKBOT, patterns in their use of postexploitation frameworks, and the ways in which they've obfuscated their BEACON payloads. Mandiant suspects that FIN12 is likely comprised of Russian-speaking actors who may be located in countries in the Commonwealth of Independent States (CIS). FIN12 has not been observed to have targeted CIS-based organisations and identified partners, and all currently identified RYUK users have spoken Russian.

Additionally, GRIMAGENT malware, which Mandiant has only observed in FIN12 incidents to date, contains Russianlanguage file resources including graphical components containing Russian text.

Fortinet Security Fabric

Broad

visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with Al-driven security for fast and efficient operations



NEW VARIANTS OF ANDROID SPYWARE LINKED TO APT C-23 ENHANCED FOR STEALTH & PERSISTENCE: SOPHOS

ophos, a global leader in next-generation cybersecurity, has published, "Android APT Spyware, Targeting Middle East Victims, Enhances

Evasiveness," detailing new variants of Android spyware linked to C-23, an advanced persistent threat (APT) adversary that has been active in the Middle East since 2017. The new variants are enhanced for stealth and persistence.

The spyware presents itself as an update app with a generic icon and name, such as "App Updates." Sophos researchers believe the attackers distribute the spyware app by sending a download link in the form of a text message to the target's phone. The first time a target runs the spyware app, it asks for permissions to control various aspects of the phone. The attackers use social engineering techniques to convince the target these permissions are essential for the app to function. After the target has granted the necessary rights, the spyware then disguises itself using the name and icon of a legitimate app. This makes it harder for the phone's user to find and manually remove the spyware.

The New Variants

The new variants use more, and more varied, disguises than previous versions, hiding behind popular app icons such as Chrome, Google, Google Play, YouTube, or the BOTIM voice-over-IP service. If targets click a fraudulent icon, the spyware launches the legitimate version of the app, while maintaining surveillance in the background.

Previous versions of the spyware relied on a single command-and-control domain that was hardcoded into the app and operated by the attackers. If a defender found and took down the domain, the spyware was disabled. Sophos researchers believe that the attackers have tried to address this potential point of weakness in the new variants, which can switch the command-and-control server to a different domain. This allows the



Pankaj Kohli, threat researcher at Sophos

spyware to continue operating even after a domain takedown.

The new variants share code with other malware samples attributed to APT C-23. Sophos researchers also found Arabic language strings in the code and observed that some of the text could be presented in either English or Arabic, depending on the language setting of a victim's phone.

Nefarious features from previous versions of the spyware remain unchanged, such as: collecting text from SMS or other apps, contacts, call logs, images, and documents; recording ambient audio and incoming and outgoing calls, including WhatsApp calls; taking pictures and screen shots using a phone's camera and recording videos of the screen; reading notifications from social media and messaging apps; and cancelling notifications from built-in security apps, as well as from Android system apps.

SOPHOS RESEARCHERS **BELIEVE THE ATTACKERS DISTRIBUTE THE** SPYWARE APP **BY SENDING A DOWNLOAD LINK IN** THE FORM OF A TEXT **MESSAGE TO THE TARGET'S PHONE.**

The spyware can also supress its own notifications.

"Spyware is a growing threat in an increasingly connected world," said Pankaj Kohli, threat researcher at Sophos. "The

Android spyware linked to APT C-23 has been around for at least four vears, and attackers continue to develop it with new techniques that evade detection and removal. The attackers also use social engineering to lure victims into granting the permissions needed to see into every corner of their digital life. Fortunately, there are practical steps that people can take to protect against spyware and many of them are worth applying even if users don't believe they're a target for surveillance."

Sophos recommends the following actions for anyone concerned about spyware or Potentially Unwanted Applications (PUAs):

Users should be wary of apps asking for sensitive permissions, such as device admin or notification access, or those requiring superuser/root access. Users can view apps with device admin and notification access permissions by browsing "Settings" and searching for "device admin apps" and "notification access," respectively

The sudden disappearance of an app icon after running it for the first time, which is often an indicator of an unwanted or malicious application

Targets of this family of spyware can remove the apps manually by navigating to the list of installed apps, selecting "Settings->Apps"and then scrolling to find the name the app used when it was first installed (such as "App Updates," "System Apps Updates" or "Android Update Intelligence")

However, many other forms of mobile malware conceal themselves from the list of installed apps. To remove these, users need the help of an anti-malware application

Sophos also advises users to install a mobile security solution, such as Intercept X for Mobile, to automatically detect spyware and malware

To avoid falling prey to malicious apps, users should only install mobile apps from trusted sources, such as Google Play. Update Android OS and other apps via Android Settings and Google Play respectively, instead of relying on third parties. ╏

CAN BLACK MATTER PUT THE RANSOMWARE GENIE BACK IN THE BOTTLE?

REVIL HAS RE-BRANDED AND COMMITTED TO SPARE CRITICAL INFRASTRUCTURE FROM ITS ATTACKS, BUT WILL THIS BE ENOUGH TO SET BACK THE RISING TIDE OF GOVERNMENT ACTION AGAINST RANSOMWARE HACKERS?

"WHAT BLACK MATTER MAY HAVE DONE THOUGH, IS BUY ITSELF – AND THE HACKING COMMUNITY AT LARGE – MORE TIME." he summer of 2021 could turn out to be pivotal for ransomware. High-profile attacks against critical infrastructure and healthcare organisations, like Colonial in the US or HSE in Europe, drove the issue to the top of everyone's agendas – including those in the corridors of power. Both the Whitehouse and the European Commission responded, which could be the start of a concerted global effort to address the ransomware blight.

These early overtures might have been enough to send waves through certain sectors of the hacking community. Within weeks, REvil appeared to have packed up, marking the end of one of the most successful ransomware operations in the world.

But, was it really the end or was this just a marketing stunt? Rising from the ashes of REvil is Black Matter, a collective bearing a startling resemblance to REvil but committing to refrain from attacking the kind of organisation that caused legislative attention to turn on its predecessor. Is a pledge only to steal from the rich enough to put the genie back in the bottle though? Or will global authorities maintain their crusade against ransomware?

At first blush, it's hard to imagine a climb down. Attacks on national critical infrastructure brought public sentiment into alignment with the long-held desire of big business for governments to act. That's a heady combination. And, having spoken out in defense of victims, how can officials roll back that stance?

Similarly, people at large have realised how vulnerable they are, and governments are on record recognising the risk. For them to now do nothing could reflect very badly in the event that a truly life-threatening attack takes place in the future.

On the other hand, many official bodies may be looking for an easy way out of a situation that's harder to deal with than they



may have first thought. No one yet has really come up with a workable plan to control ransomware through legislation.

Banning payment isn't the easy solution it may seem. Outlawing the payment of ransoms could force hackers to focus in on those organisations that would have to pay, even in defiance of the law. For example, hospitals who are forced to choose between payment or letting people die for lack of access to their records or medical apparatus. Equally, banning payment wrongly criminalises the victim. It's akin to making it illegal to surrender your cash if someone mugs you. You can't send someone to jail for someone else's criminal attack.

And the alliance of public and business goals is likely to be short lived if Black Matter is able to position itself as a kind of "cyber Robin Hood" – albeit one that robs from the rich without actually giving anything to the poor. Public outcry is likely to wane without the queues trailing to the petrol stations or the empty supermarket shelves.

Realistically though, can Black Matter live up to the brand that it wants to create for itself? With the best will in the world, once you've created a monster, you can't expect to be able to control it. So, even if Black Matter doesn't intend to attack critical infrastructure, it can't guarantee that its malware won't end up taking down a power station.

And the promise to release the encryption code for free to any accidental victims of this nature isn't exactly the silver bullet they might make it out to be. How quickly could a hospital expect to be up and running again, even with the decryption code? It's unlikely to fast enough to avoid any harmful consequences.

For this reason alone, it seems like it's going to be impossible for Black Matter to put the genie back in the bottle altogether. A future attack on critical infrastructure is almost inevitable and the international community has to act to protect against that.

What Black Matter may have done though, is buy itself – and the hacking community at large – more time. Taking the edge off of the urgency of action gives policy makers time to breathe and think through their options.

And that time is all that the hackers need in order to keep their scams going with businesses that drive their income. Organisations should be prepared to continue to take responsibility for their own protection for a good while yet, which means doubling down on security and data protection.

UNDERSTANDING NUMBER Image: Constant of the standard state of the standard state of the state

hat do you see as the key trends in market? Digital transformation, COVID, and more

sophisticated cyber adversaries in dynamic and more complex IT environments will continue to be trends worldwide.

> **"FIDELIS CYBERSECURITY HAS ALWAYS MAINTAINED A STRATEGY OF** PRESERVING **RESOURCES CLOSE TO** OUR CUSTOMERS AND **PARTNERS, FIDELIS** WILL ADDRESS AND WORK CLOSELY WITH **COMPANIES LOOKING** TO ADD PROACTIVE CYBER DEFENSE CAPABILITIES TO BETTER SAFEGUARD **THEIR DATA, ASSETS AND SERVICES.** ⁴

Digital transformation enables massive scalability and agility, as well as cost advantages. But it also increases IT complexity. SOC teams need to ensure data and assets are secure no matter where they reside on your networks.

While digital transformation has dispersed data to new place, COVID has pushed our people to working from new places. Instead of securing one corporate environment with 500 people, we're securing 500 "offices" of one person each. Classic phishing tactics thrive on naivety. COVID also limited budgets and the resources we have available.

Cyber adversaries are getting more sophisticated and are using more advanced tools, neural networks, Al tools, automated analytics to achieve their goal. They have found new ways in, penetrate environments deeper and linger longer. These threat actors are bringing global organizations and supply chains to a halt.

In short, complicated environments, limited resources, against very wellprepared adversaries is yielding 1M new threats discovered in the world every day.

Modern cyber defenders/security teams must have deep visibility across hybrid and multi-cloud environments coupled with rich analytics to protect all data, assets, and services and better safequard their IT environment.



What expansion and growth plans do you have for the region? What are the priorities for customers?

Fidelis Cybersecurity has always maintained a strategy of preserving resources close to our customers and partners. Fidelis will address and work closely with companies looking to add proactive cyber defence capabilities to better safeguard their data, assets and services. That strategy means we will continue to invest in local resources based in the region, as well in local partner ecosystem. Quality alliances in the region are critical to our business success. We will continue knowledge transfer and trainings locally to enrich existing and simplify new partnerships and provide customers and partners the tools they need for success.

What strategic relationships are important to you in the region?

Fidelis Cybersecurity recently sign very strategic and important local MSSP

partnerships to help customers who want the value we offer delivered as a service. Work closely with these MSSPs to develop and deliver a unique managed security services value-based offering, and this will continue to be a key priority in the local market.

Can you tell us about the roadmap for Fidelis Cybersecurity and the value it will provide to customers?

Fidelis Cybersecurity portfolio is designed to deliver the proactive defence capabilities you need to safeguard your data, assets, and services – no matter where they are on your networks. Already, we provide proactive and defence-in-depth security that spans endpoints, network, and hybrid and multi-cloud environments.

We acquired CloudPassage in May, which is allowing us to further evolve our XDR platform with a solution that keeps pace with our customers' needs as they migrate more and more of the business to the cloud. Our customers have a choice to use our XDR platform as a comprehensive offering, or they can deploy it as an open platform leveraging integrations with existing tools in their environment. We will continue to deliver integrations and functionality our customers need from an Active XDR platform to detect, respond, and neutralize threats earlier in the attack lifecycle.

Finally, cyber threats succeed when they can detect and exploit risks and vulnerabilities. Fidelis starts by understanding the current environment and risk, allowing the security team to address risk prior to an exploit. Risk has traditionally been based on vulnerability scans that are run periodically - daily or weekly, however risk changes immediately when threats are activated - through phishing, malware, user impersonation, etc. We will combine detections from endpoint, network, and cloud in a way that immediately changes risk, automatically responds, and constantly evolves the security of the enterprise.

What do you see happening with the cloud and on prem offerings and private cloud?

Digital transformation is happening. Data centers are moving to the cloud. Security needs to also move. These hybrid environments are more complicated to secure, and each enterprise must decide for themselves how to proceed. If they decide to use on-prem data centers, private cloud or public cloud, security must view this as a deployment strategy without any loss of capability. Fidelis will allow our customers to deploy security to match their enterprise environment, including cloud, on-prem, or hybrid without loss of detection capabilities. **1**

REVISIT THE FUNDAMENTAL ELEMENT OF SECURED BANKING: KNOW YOUR BREACH LIKELIHOOD

SAKET MODI, CO-FOUNDER & CEO AT SAFE SECURITY



an I jump over two or three guys like I used to? No. Am I as fast as I used to be? No, but I still have the fundamentals and smarts. That's what enables me to still be

a dominant player. As a kid growing up, I never skipped steps. I always worked on fundamentals because I know athleticism is fleeting — Kobe Bryant

For any discipline — be it sports, music or academics — the grasp on fundamentals needs to be strong. One cannot, after all, write a sentence without first learning the alphabet.

The pandemic has catalyzed digital changes within organizations and outside them as their customers embraced open banking and digital transactions. According to Business Insider Intelligence's Mobile Banking Competitive Edge study, 89% of survey respondents said they use mobile banking. Deloitte reports that 35% of customers increased their online banking usage during Covid-19, and Visa saw about 13 million Latin American customers make their first online transaction in the first guarter of 2020.

With such a digital boom, cybersecurity has come into sharp focus. However, the fundamentals of how cybersecurity is approached are still unclear, which is why we still see businesses spend on the bottomless well and still get breached.

According to a Deloitte report, financial institutions are expected to spend roughly 11% of their IT budget on cybersecurity, with the largest banks in the U.S. investing \$1 billion each! However, while organizations are improving in cyberattack planning, detection and response, their ability to contain an active threat has declined by 13%, according to IBM's Cyber Resilient Organization Report.

What Are the Fundamentals?

Currently, the five vectors of the banking sector — people, processes, technology, third-parties and cybersecurity products - are viewed in silos and treated as such. People, security, security tools, compliance and audits are considered fundamental to cybersecurity when they are a part of a granular picture. Organizations are purchasing more products to generate more lists, based not on objective measurements but subjective abstractions of the CIO, security team or competitor enterprises. On average, enterprises deploy 45 cybersecurity-related tools. However, there is a definite lack of cohesiveness in determining what is going well and what could be better. To put it in perspective, enterprises that deploy over 50 cybersecurity tools rank themselves 8% lower in their ability to detect threats than other companies employing fewer toolsets!

There is no industry standard determining the fundamentals enabling financial institutes (FI) to answer one simple question: How secure are they today? When the CEO can be held accountable for an organization's breach (as per the GDPR), the board gets more curious and involved in the decision-making processes of cybersecurity than ever before. In such a scenario, cybersecurity should transform from being jargon-rich to simple, unified and easy. Managing, mitigating and measuring risk objectively is the fundamental shift required, and this comes with the knowledge of an enterprise's breach likelihood.

Financial Institutions Needed to Adopt Breach Likelihood Yesterday

Gartner defines integrated risk management (IRM) as "practices and processes supported by a risk-aware culture and enabling technologies, that improve decision making and performance through an integrated view of how well an organization manages its unique set of risks."

The building block of IRM is enterprise risk. Currently, organizations have tried and failed to protect data by looking at cybersecurity through compliance frameworks only, with point-in-time reports from siloed tools. It is time they move from reactive and defensive risk management to predictive risk management through breach likelihood, which simplifies cybersecurity.

Computing an enterprise's breach likelihood leverages technology that is not alien to the BFSI sector. Machine learningenabled predictions are already being deployed in insurance, employee welfare and customer experience. A large online payments system uses deep learning, algorithms, multi-class models and more to sieve fraudulent and genuine transactions by deriving actionable insights from their story-model analysis.

Cybersecurity can also be simplified

"THERE IS NO INDUSTRY STANDARD DETERMINING THE FUNDAMENTALS ENABLING FINANCIAL INSTITUTES (FI) TO ANSWER ONE SIMPLE QUESTION: HOW SECURE ARE THEY TODAY?" using technology that already exists. The fundamental element of cybersecurity is as basic as knowing the enterprise breach likelihood that can be calculated from enterprise-wide signals. Breach likelihood prediction in the banking sector shifts power to the cybersecurity team and the organization, enabling them to prevent rather than react to threats. Be it the possibility of a breach through ransomware, cloud misconfigurations or business email compromise, breach likelihood gives an as-is metric for cyber risks and a means to prioritize vulnerabilities. This simplifies the understanding and management of cybersecurity.

FIs willing to invest in methods that simplify cybersecurity can begin with:

• Stepping away from a complianceonly qualitative approach to ensure no vectors — people, processes, technology or cybersecurity products for both first and third parties — go unaddressed.

• Consolidating reports from all cybersecurity products/services to a single dashboard. This will help security and risk management teams prioritize risks across the enterprise in a single view.

• Measuring their cyber risk posture in its as-is state. They either accept the risk and improve their risk posture by purchasing cyber insurances, accept the risk and forgo any changes, especially when the investment required to mitigate the risk is larger than its dollar value impact, or mitigate the vulnerabilities by defining their cyber risk appetite and cyber risk tolerance.

To date, the fundamental approach of securing any business has been reactive. Investments in cybersecurity have historically maintained a check-the-box approach to meet compliance and audit requirements. There are many distractions and abstractions surrounding cybersecurity, especially when it is a qualitative analysis. Once the foundation is solid with an industry-wide breach likelihood adoption, cybersecurity will become a solution rather than a problem that security executives perceive as right now. **1**

HOLIDAY SEASON POSES SECURITY CONCERNS FOR UAE ORGANIZATIONS, SAYS MCAFEE ENTERPRISE & FIREEYE REPORT

<section-header><section-header><complex-block>

and FireEye have released a research titled Cybercrime in a Pandemic World: The Impact of COVID-19, revealing the imminent need for organizations in the UAE, and across the globe, to prioritize and strengthen their cybersecurity architecture. The findings indicate that during the pandemic, 87% of UAE organizations experienced increased cyber threats, with

cAfee Enterprise

83% experiencing downtime due to a cyber incident during a peak season. As the holiday season approaches, supply chain and logistics, ecommerce and retail, and travel industry see predictable increases in consumer and business activity, making them more vulnerable to cyber threats and leaving UAE businesses, employees and consumers' data at risk.

"It is imperative all businesses prioritize security technology to keep them protected, especially during the peak holiday season," said Bryan Palma, CEO of the newly combined company. "Most IT professionals want their organization to improve its overall cyber readiness. Businesses must do more and need an intelligent security architecture for managing today's sophisticated threat landscape."

Supply Chain & Logistics

According to BCI's Supply Chain Resilience Report 2021, 27.8% of organizations reported more than 20 supply chain disruptions during 2020, up from just 4.8 percent reporting the same number in 2019. The loss of manufacturing and logistics capacity and employee-power, paired with increasing demand for goods, has created the perfect attack vector for cybercriminals: a potentially weak and vulnerable infrastructure to break through. Supply chain managers must identify risks, understand the potential downstream effects of a security breach or cyberattack, and prepare response plans so that they can act quickly in the event of an incident. **Ecommerce & Retail**

According to Adobe's 2021 Digital Economy Index, global online spending is expected to increase by 11% in 2021 to \$910 billion during the holiday season. With store closures and increases in online shopping, along with limited product availability and concerns about shipping, this industry is faced with more threats than before. According to McAfee Enterprise COVID-19 dashboard, the global retail industry accounts for 5.2% of the total detected cyberthreats.

Travel

Cyber threats aren't new to the travel industry – airports, airlines, travel sites and ride sharing apps have been victims in years past. However, this industry has been in a holding pattern because of travel restrictions. According to the International Air Transport Association (IATA), coronavirus-related loss estimates for 2020 total \$137.7 billion—with total industry losses in 2020-2022 expected to reach \$201 billion.

Addressing Emerging Threats

There are ways for organizations to be proactive and actionable against cybercrime, such as implementing security measures and industry-wide cybersecurity requirements, providing cybersecurity awareness training for employees, and developing prevention and response plans. In addition, enterprises and commercial business can implement cloud-delivered security with MVISION Unified Cloud Edge (UCE) and FireEye Extended Detection and Response (XDR).

VIRSEC Protect Your Software as it Runs.

To fully protect your software, you must first fully understand it. Only Virsec can do this, by creating a dynamic golden image of what your software is supposed to do—and immediately stop anything that it's not.



Stop Fileless Memory Attacks | Protect Legacy Applications | Reduce Patching Urgency | Engineered for Servers—Not Endpoints

"We are at the inflection point for the next paradigm shift in cybersecurity and Virsec does what is needed: protect application workloads at runtime. This is the new battleground." – John Chambers, Virsec Investor and Strategic Advisor and Former Cisco CEO

We invite you to learn more: virsec.com | info@virsec.com

Experience SELF-OPTIMIZING Wi-Fi, powered by Al

IREA

D-Link EAGLEPROAI

One Connection - Infinite Possibilities



amazon alexa

With advanced AI features for continuous network monitoring, the R15 keeps your Wi-Fi performing at its best. Managing your network has never been easier with the AI Assistant on the free mobile app.

R15 AX1500 Smart Router



AI Parental Controls

AI Mesh Optimizer

AI Wi-Fi Optimizer



AI Assistant



AI Traffic Optimizer



EAGLE PRO AI



https://me.dlink.com Connect to more...