

Security

ADVISOR

MIDDLE EAST

SPOTLIGHT:
GISEC

ANATOMY OF AN OT ATTACK

MAHER JADALLAH, SENIOR DIRECTOR - MIDDLE EAST & NORTH AFRICA, TENABLE, ON WHY A PREVENTIVE APPROACH TO CYBER-ATTACKS IS ALWAYS MORE SUSTAINABLE.

Fortifying IT for today, and tomorrow.

- » Over 300,000 customers in 190 countries from SMB to Fortune 500®
- » 499 of the Fortune 500 are customers
- » #1 in Network Management*
- » 50+ IT management products

solarwinds.com

IT forward 

Come visit us at GISEC!

May 31 - June 2 | Booth SS3-B1



NETWORK
MANAGEMENT



SYSTEMS
MANAGEMENT



SECURITY AND
COMPLIANCE



IT SERVICE
MANAGEMENT



DATABASE
MANAGEMENT



APPLICATION
MANAGEMENT



06 **NEWS**
We bring you the latest from the world of cybersecurity.

22 Mika Lauhde, Vice President of Cybersecurity & Privacy – Global PACD, Huawei, discusses how Huawei works together with customers, partners, standards organisations and other industry players in the Middle East region to elevate its ICT industry to the next level.

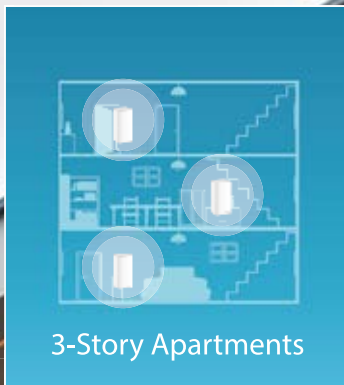
24 Jihad Tayara, CEO of EVOTEQ, on viewing security as a part of an organisation's digital transformation journey.

28 GISEC SPECIAL: A round-up of what to expect at GISEC 2021, with the spotlight on some of the participants.

38 Werner Gevers, Regional Manager, Mimecast Middle East, on why organisations today need a security strategy that's as pervasive and persistent as the threats they work to combat every day.

Simple. Yet Flexible

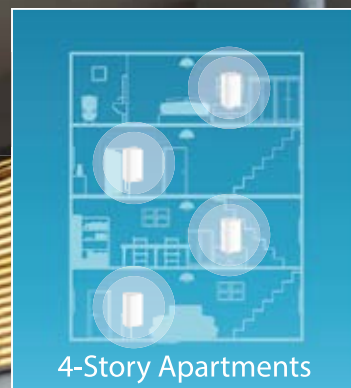
Wi-Fi 6



3-Story Apartments



**COVR-X1873
(3-pack)**



4-Story Apartments



**COVR-X1874
(4-pack)**

AX1800 Whole Home Wi-Fi 6 Mesh System



Smart Roaming



MU-MIMO Technology



Smart Steering



Simple Setup



Profile-based Parental Controls



Expandable Network



WPA3™ Encryption



Works with your existing router or gateway



Connect to more...

D-Link®

EDITORIAL



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

Anita Joseph
Editor

COMBATING CYBERCRIME

It's that time of the year again: GISEC, one of the most anticipated and impactful cybersecurity expo and conferences in the region, is gearing up for an exciting new edition, right here in Dubai. This year is even more special, because this live, in-person event is a testament to the human spirit of resilience and courage in the face of adversity.

Despite the pandemic still wreaking havoc in many parts of the world, GISEC promises to bring together some of the world's most prominent InfoSec and tech professionals, business leaders, change makers and senior practitioners for three days of unparalleled discovery, learning & networking. With thousands expected to attend, the venue is expected to come alive with the latest in the world of security and cybercrime prevention.

This issue of Security Advisor Middle East is dedicated to this mega-event and all those who make it happen. In fact, we

have set apart a special section focused on the event, with a sneak-peek into what to expect, and some of the participants telling us what they look forward to.

But if you thought that was all, you're mistaken: we've lined up some of the most important news and views from the

world of cybersecurity and the ever-growing threat landscape.

We have global players such as Anomali, Tenable and Mimecast giving us valuable insights into the inside story of how attacks happen and what can be done to prevent them. We also have opinion pieces and spotlight articles on the latest technology products & solutions that ensure maximum protection and security.

There's never a dull moment in this issue of your favourite magazine. It will delight and inform you as you browse its pages, with plenty to keep you hooked. So happy reading, see you at GISEC!

**THIS YEAR,
GISEC IS EVEN
MORE SPECIAL
AS IT HELPS TO
BRING ABOUT A
SEMBLANCE OF
NORMALCY TO THE
EVENTS SPACE
AND STANDS AS A
TESTIMONY TO THE
HUMAN SPIRIT OF
RESILIENCE.**

EVENTS



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

Published by



Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

**EDITORIAL
Editor**
Anita Joseph
anita.joseph@cpimediagroup.com

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

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

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

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

**DIGITAL SERVICES
Web Developer**
Adarsh Snehan

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

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

© Copyright 2021 CPI
All rights reserved

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

MCAFEE BREAKS THROUGH XDR MARKET WITH SASE-ENRICHED THREAT PROTECTION TO PROACTIVELY STOP TARGETED ATTACKS



McAfee Corp. the device to cloud

cybersecurity company, has announced significant expansion of its MVISION Extended Detection and Response (XDR) solution by correlating the extensive telemetry of McAfee's endpoint security solution, Secure Access Service Edge (SASE) solution, and threat intelligence solution powered by MVISION Insights.

These integrations protect organisations against the most advanced threats while simplifying security operations with unified control and visibility from device to cloud. McAfee MVISION XDR is the first proactive, data-aware, and open XDR platform designed to help organisations stop these sophisticated, multi-vector attacks with unified threat detection and response that

connects and fuses disparate endpoint, network, and cloud data sources. Starting today, XDR incidents are enriched with actionable threat insights from McAfee's SASE solution, which detects cloud threats that occur within web and SaaS environments. It improves situational awareness, drives better and faster decisions, and elevates the SOC to a new level of efficiency and effectiveness.

"SOC processes involve siloed monitoring and detection tools that generate an overwhelming volume of security alerts that often require manual effort to sort through and force analysts to take a reactive posture," said Shishir Singh, chief product officer of McAfee's enterprise business. "AI Guided Investigations serves as the catalyst allowing analysts to more effortlessly orchestrate smart and efficient workflows. MVISION XDR delivers end-to-end threat visibility across all attack surfaces, greater context, and situational awareness using automation to streamline operations so organisations can preempt an attack rather than scramble to contain a breach," he added.

MVISION XDR is available today.

SPIRE SOLUTIONS VENTURES INTO THE BIG DATA & ANALYTICS DOMAIN

The world has moved towards digital

economies driven by data and artificial intelligence (AI). Both public and private sector organisations have started relying heavily on the power of data and the intelligence that can be derived from it to transform their service/business and make better decisions.

Data is set to grow faster than ever with 1.7 MB of data currently being created every second for every human being on the planet (as per Forbes). It's estimated there will be 50 billion intelligently connected devices globally in five years, all developed to collect, analyse, and share data.

As per Market Research, the Middle East & African AI, Big Data Analytics & Cyber

Security Market value was USD 11.78 billion in 2020, and it is expected to reach USD 28.36 billion by 2026. Yet, reliable and scalable data solutions, services, and consultants are far and few in the region.

To address this gap and help resolve big data and data analytics challenges, the region's leading value-added distributor Spire Solutions is launching its Big Data and Data Analytics business unit. The Business Unit will be led by a fully qualified team with over a decade's experience in the data spectrum and empowered by strong partnerships with niche vendors specialised in data science, AI, and data monetisation.

Mohieddin Kharnoub, Chief Revenue Officer at Spire Solutions said "We

MOHIEDDIN KHARNOUB, CHIEF REVENUE OFFICER AT SPIRE SOLUTIONS



are excited for launching our Big Data and Data Analytics unit which help our customers in their end-to-end data journey. Right from solving complex data engineering scenarios to building modern-day AI-driven analytics solutions, our goal is to make data matter and monetise it".

Spire will soon be announcing its collaboration and strategic alignment with leading data technologies and run a series of awareness sessions for the benefit of business and technology decision-makers across the Middle East & Africa.



CYBERKNIGHT BECOMES FIRST LOOKOUT VAD IN MIDDLE EAST TO EXTEND ZERO TRUST SECURITY TO CLOUD

WAEEL JABER, VP
TECHNOLOGY
& SERVICES,
CYBERKNIGHT

With the rapid adoption of cloud across

the region, especially due to the dramatic growth in remote working, organisations need to protect their data and IT systems from cloud-based threats more than ever. Gartner forecasts that over the next five years, the SASE market will grow at a CAGR of 42%, reaching almost \$11 billion by 2024. In addition, Gartner predicts that spending on Cloud Access Security Broker (CASB) solutions will grow 40.7% in 2021, 36.7% in 2022 and 33.2% in 2023, outpacing all other information security markets.

To address customer challenges related to cloud security including cloud access, discovery, monitoring, data protection, policy enforcement and compliance, CyberKnight has signed a partnership agreement with Lookout, an integrated endpoint-to-cloud security company to distribute its products in

Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates. The Lookout Secure Access Service Edge (SASE) solution delivers the market's leading approach to integrated Mobile Endpoint Security, Zero Trust Network Access (ZTNA), and Cloud Access Security Broker (CASB).

Lookout Mobile Endpoint Security Lookout was named a leader for the third year in a row in the 2020 IDC MarketScape for Worldwide Mobile Threat Management Software, and a representative vendor for the fifth year in a row in the 2021 Gartner Market Guide for Mobile Threat Defense. Lookout CASB, the newest addition to the company's product portfolio through its March 2021 acquisition of CipherCloud, was named an overall Leader in the KuppingerCole Market Compass: CASB 2021, and positioned as a visionary in the 2020 Magic Quadrant for CASB by Gartner.

"Undoubtedly, the cloud is an expanding threat vector and

organizations of all sizes require a robust security platform to mitigate the risks of data loss and exposure. With Lookout, CyberKnight is now able to offer organisations enterprise-class visibility and protection across their cloud environments. We have joined forces with the industry expert in SASE specifically to eliminate data privacy, security and sovereignty risks that can often derail cloud projects, especially in the Middle East," commented Wael Jaber, VP Technology & Services, CyberKnight.

"The Lookout SASE solution eliminates the top concerns impeding cloud adoption – security, data privacy, monitoring, and regulatory compliance. We are excited about our new partnership with CyberKnight and look forward to leveraging its strategic partner network to help ensure regional enterprise and government organisations are secure at the endpoint, in the cloud and everywhere in between," said Wim van Campen, Head of EMEA Sales, Lookout.

AMIVIZ LAUNCHES FIRST EVER ENTERPRISE B2B MARKETPLACE FOCUSED ON CYBER SECURITY INDUSTRY IN MIDDLE EAST



As the world moves faster towards

digital economy and digital transformation gaining ground in past one year due to COVID-19, it is important that businesses also follow suit and be ready to embrace the digital world.

AmiViz took up the challenge and developed the region's first B2B e-commerce platform with a human touch for the cyber security industry to serve the channel ecosystem by automating the entire business process. AmiViz is a one-of-a kind enterprise

marketplace specially designed to benefit both the channel partners and vendors with this initiative. The new platform with its collaborative tools help channel partners to scale up their operations and enable them to expand their reach as well as tailor better deals for their customers.

AmiViz platform offers a unique customer experience for the channel by taking away their pain points and streamlining the processes to ensure efficiencies. This will allow partners to save time and money and to be well-informed with cyber security trends and opportunities in the region. The new marketplace introduces ease of doing business and enabling channel

partners to provide remote POCs and demonstration, track their inventory, view orders and payments.

Besides providing a consumer styled e-commerce platform experience, AmiViz also offers value added services and consultancy thereby maintaining the human touch that is critical to the entire ecosystem and supporting the channel partners.

In an age of shrinking margins, AmiViz reinvents the business of channel by eliminating the human bias and errors and enable partners to leverage data to help in every aspect of the business by increasing efficiency and reducing the cost of transactions that will accelerate profitability for the channel.

SOPHOS UNVEILS XGS SERIES FIREWALL APPLIANCES WITH INDUSTRY-BEST TLS INSPECTION

DAN SCHIAPPA,
CHIEF PRODUCT
OFFICER AT SOPHOS



Sophos, a global leader in next-generation cybersecurity, has unveiled new XGS Series firewall appliances with unrivaled performance and advanced protection against cyberattacks. The new appliances feature industry-best Transport Layer Security (TLS) inspection, including native support for TLS 1.3, that is up to five times faster than other models available in the market today.

"Sophos Firewall XGS Series appliances represent the most significant hardware upgrade that we have ever released and introduce unmatched detection, protection and speed," said Dan Schiappa, chief product officer at Sophos. "Security teams can no longer afford to overlook encrypted traffic for fear of breaking something or hurting performance – there's too much at risk. We've completely redesigned the Sophos Firewall hardware to handle the modern encrypted internet. Security teams now have the ability to easily inspect encrypted traffic and shine light on what was once a black hole, and they can confidently do so without compromising on performance."

Powered by Sophos Firewall's Xstream architecture, XGS Series appliances deliver the industry's best zero-day threat protection, identifying and stopping the most advanced known and potential threats – including ransomware. Protection is fueled by powerful threat intelligence, available only through SophosLabs Intelix and based on petabytes of SophosLabs threat data. Suspicious files are safely detonated in SophosLabs Intelix virtual environments as well as subjected to in-depth static analysis for additional detection coverage and intelligence gathering.

THREATQUOTIENT LAUNCHES DATA-DRIVEN APPROACH TO SOAR AND XDR, ACCELERATING DETECTION & RESPONSE

ThreatQuotient, a leading security operations

platform innovator, has announced ThreatQ TDR Orchestrator, a new data-driven automation capability for more efficient and effective threat detection and response. This capability enables users to control what actions are to be taken, when, and why through the use of data.

"The security industry's approach to automation has overlooked the vastly different needs of detection and response use cases," said Leon Ward, VP of Product Management, ThreatQuotient. "The focus of ThreatQ TDR Orchestrator is data, not process. In detection and response, what is learned when performing an action is far more important than the action itself. ThreatQuotient has seized an opportunity to define and provide automation in a way that reduces complexity for security teams."

ThreatQ TDR Orchestrator puts the "smarts" in the platform and not the individual playbooks by using Smart Collections™ and data-driven

LEON WARD, VP OF
PRODUCT MANAGEMENT,
THREATQUOTIENT



playbooks. The application of Smart Collections and data-driven playbooks provides for simpler configuration and maintenance, and provides a more efficient automation outcome. This approach further addresses all three stages of automation – Initiate, Run and Learn – easily and efficiently by enabling users to curate and prioritize data upfront, automate only when relevant, and simplify actions taken. It can be used to complement other playbook capabilities through ThreatQuotient's ecosystem partners or users can define data-driven playbooks within the ThreatQ platform. To improve the platform "smarts", it will also capture what has been learned to improve data analytics, which in turn improves the initiation stage of automation.

ThreatQ TDR Orchestrator will be available in Summer 2021.

SENETAS AND THALES LAUNCH WORLD'S FIRST QUANTUM RESISTANT NETWORK ENCRYPTION SOLUTION



Thales and Senetas

have collaborated to launch the world's first quantum resistant network encryption solution, capable of

protecting customer data (at speeds up to 100 Gbps) against future quantum attacks. Regarded as among the most significant threat to cybersecurity, quantum-computing looks set to render many of today's security methods, such as encryption, obsolete.

Enabling customers to combine both conventional and quantum resistant encryption in a single network security platform, the solution also provides long-term data protection in a quantum world. Hackers harvesting encrypted data today, will come unstuck when attempting to break data with supercomputing power in the future. The adoption of the new standards will protect any critical data and continue to render the data useless without the correct key.

"As quantum computing becomes a reality, organisations around the world should develop a quantum security strategy and start planning to implement quantum resistant encryption sooner rather than later. This is the first to market high-speed network encryption platform that provides quantum resistant encryption with today's encryption technology. Our government, defence and business customers can make a secure transition to a future quantum-safe world knowing data is protected for the long-term", said Andrew Wilson, Senetas CEO.

"It's vital that businesses understand that all of today's encryption standards are not fit for a quantum world. Hackers know quantum is coming and are actively working to steal data now so they can access it in the future, and large and multi-national organisations are most at risk due to compliance and privacy mandates. Businesses can't afford to wait, the time is now to review their security quantum strategy", said Todd Moore, Vice President, Encryption Solutions at Thales.

FORTINET EXTENDS SECURITY FABRIC WITH NEXT-GEN FIREWALL AND 5G

JOHN MADDISON, EVP
OF PRODUCTS AND
CMO AT FORTINET



Fortinet, a global leader in broad, integrated and automated cybersecurity solutions, has announced the new FortiGate 7121F and FortiExtender 511F-5G to further secure and accelerate 5G adoption. Powered by Fortinet's proprietary SPU ASICs, the FortiGate 7121F delivers the highest-performing security necessary for 5G networks and enterprise Zero Trust Access, while FortiExtender 511F-5G provides wireless WAN connectivity for SD-WAN and SASE solutions.

"Fortinet has heavily invested in the development of its 5G security portfolio. Delivering the world's fastest NGFW, we help service providers secure radio and Internet interfaces at

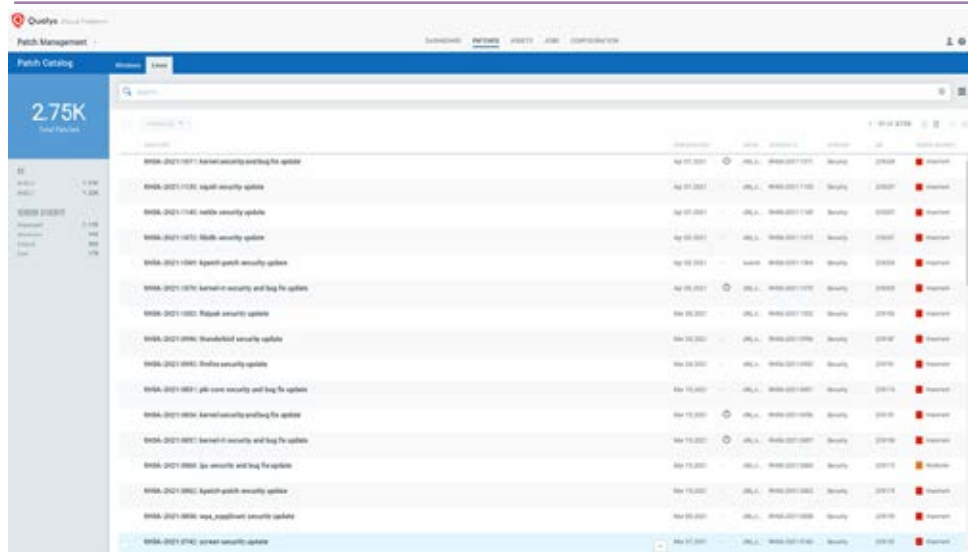
price performance numbers 10 times today's benchmarks. Additionally, the new 5G FortiExtender provides more WAN connectivity options and is fully integrated into the FortiGate SD-WAN policy engine," said John Maddison, EVP of Products and CMO at Fortinet.

5G will enable transformation and innovation for both the enterprise and mobile network operators (MNOs). To unleash its full potential, a new 5G ecosystem, including operational technology (OT) and industrial control vendors and public cloud vendors, is being formed to create new sets of applications and services that will drive this transformation for the industrial enterprise.

This expanded 5G ecosystem

introduces additional edges and expands the digital attack surface, posing new cybersecurity risks. To address this challenge, the new FortiGate 7121F consolidates networking and security through a security-driven networking approach to deliver full visibility, the highest scalability and advanced security to protect business-critical applications in the distributed and hybrid 5G ecosystem. Through the breadth of the Security Fabric, Fortinet provides end-to-end security for 5G private and public network ecosystems, while also providing flexible connectivity and threat intelligence capabilities.

QUALYS EXTENDS VMDB TO PATCH LINUX WORKLOADS



Qualys, Inc, a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, has announced it is continuing to expand its vision of providing vulnerability detection and response through a single platform, thus reducing the time it takes to fix vulnerabilities, with the

inclusion of patch support for Linux systems. With this addition, Qualys Patch Management now supports patching for Linux, Windows and third-party apps from the same console with a common workflow.

Available as part of the VMDB solution, Qualys Patch Management

is a complete cloud-based solution that helps security and IT professionals streamline and accelerate vulnerability remediation for Linux and Windows operating systems as well as mobile and third-party applications.

"Adding Linux patching to VMDB builds on Qualys' promise to automate detection and orchestration of the entire vulnerability and patching process so that customers can significantly accelerate time to remediation and enhance their overall security posture," said

Sumedh Thakar, interim CEO and chief product officer, Qualys. "In addition to providing a unified view for patching both Linux and Windows operating system, the end-to-end approach to vulnerability management eliminates silos between security and IT teams and speeds up the remediation process."



MICRO FOCUS: OFFERING DRAMA-FREE IT WITH OPTIC

TOUFIC DERBASS, MANAGING DIRECTOR MICRO FOCUS MIDDLE EAST & AFRICA, DISCUSSES HOW THE LATEST IT PLATFORM FROM MICRO FOCUS OFFERS UNIFIED INTERFACE AND & EXPANDED INTEGRATION CAPABILITIES.

OPTIC IS DESIGNED TO WORK WITH YOUR EXISTING INFRASTRUCTURE AND SERVICES SO YOU CAN BUILD ON YOUR INVESTMENTS, RATHER THAN RIPPING AND REPLACING.”

Micro Focus, a worldwide leader in software solutions, continues to deliver on its promise of “digital

transformation without the drama” with the launch of its new IT platform, OPTIC (the Operations Platform for Transformation, Intelligence, and Cloud). OPTIC is a unified platform and automation engine that requires no custom coding and offers embedded intelligence for broad data analysis, normalisation, and storage.

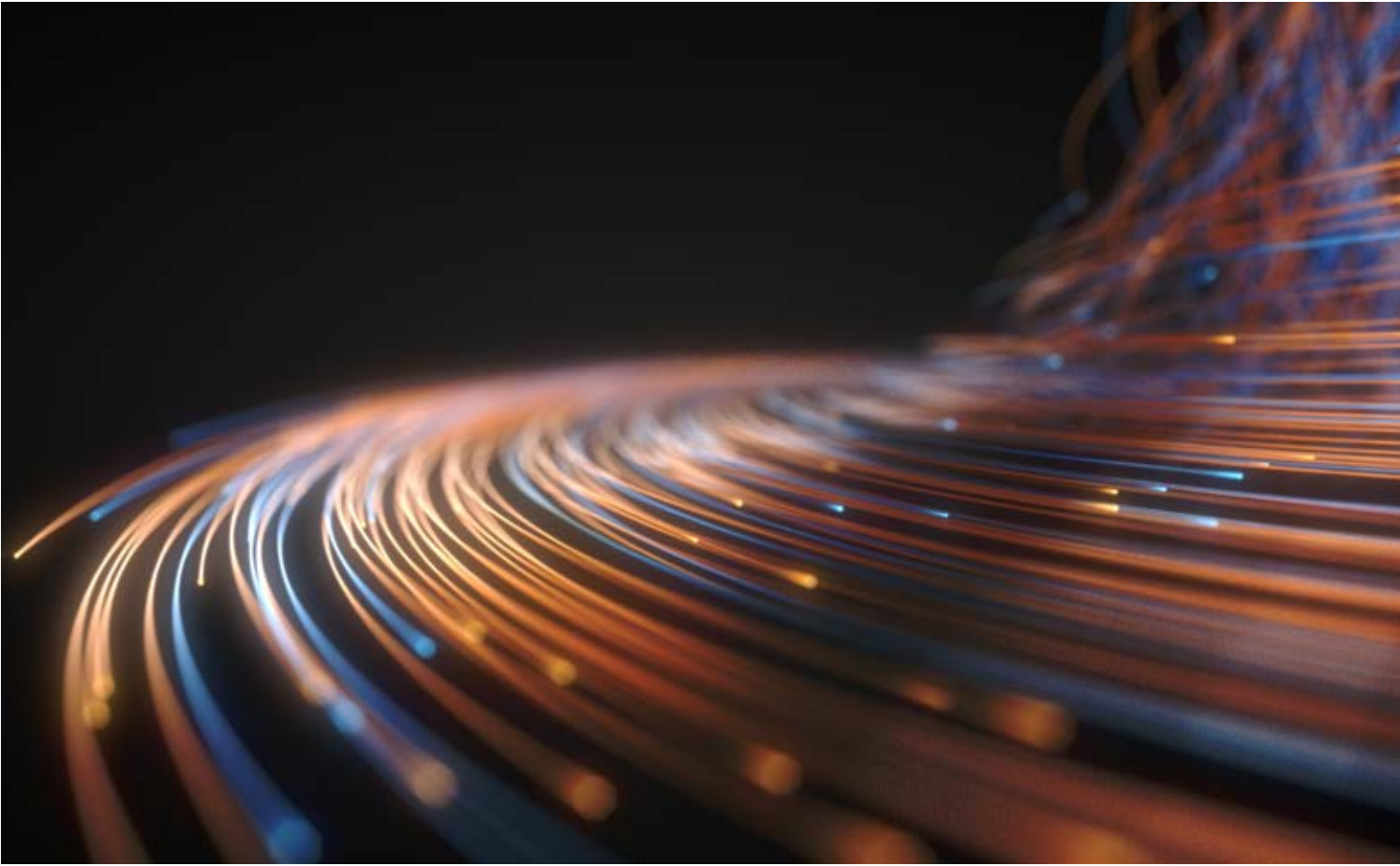
The platform’s new features reflect the changing IT demands of businesses and their employees. OPTIC streamlines disparate needs and services, with a unified approach to identity management, single-sign on, and container management. The next-generation IT platform has

expanded integration capabilities through an API gateway and harnesses a native, unlimited-use intelligence at its core that allows teams to optimize their cloud usage.

At Micro Focus, our goal is to take the drama out of digital transformation so organizations can get the most from their investments and focus on driving business forward. OPTIC is designed to work with your existing infrastructure and services so you can build on your investments, rather than ripping and replacing.

Control your transformation journey

OPTIC allows teams to take control of their digital transformation. The platform provides efficient self-service for employees with features like automated fulfillment which cuts down on processing time and does away with long waits for simple requests. With



OPTIC, teams can discover, manage, monitor, and govern cloud services while maintaining an on-premise approach. Fully integrated with the cloud, OPTIC can unify performance and availability management, while at the same time discovering

**OPTIC TAKES THE
DRAMA OUT OF THE
IT PLATFORM SO
BUSINESSES CAN
SPEND MORE TIME
LEVERAGING THE
TOOL AND LESS TIME
TWEAKING AND
TRAINING.”**

new possibilities with multi-cloud deployment options.

“Having an IT platform is crucial in today’s environment, but not all platforms are the same. OPTIC reduces the need to build and maintain integrations, provides deep insights into data and processes, and leverages a common UI and best practices so users can work on a familiar, optimised platform,” says Derbass.

“Simply put, OPTIC takes the drama out of the IT platform, so businesses can spend more time leveraging the tool, and less time tweaking and training.”

Build more, spend less

Keeping expenditures low is essential in today’s uncertain business environment. OPTIC is built for integration and supports existing IT infrastructure and services, both on-premise and in the cloud. Businesses that choose OPTIC need not replace

valuable workhorse systems like business intelligence and reporting tools, and can instead leverage previously adopted investments while improving operational efficiency. OPTIC deployment options include cloud, containers, as-a-service, or on-premise, as well as the ability to switch as business needs evolve. Additionally, OPTIC components are licensed and installed with Micro Focus ITOM products, providing incremental value to customers as they expand their use.

OPTIC is one more way Micro Focus is taking the drama out of IT transformation and getting the most out of existing investments. With unified process automation, discovery and topology mapping, and embedded intelligence all in a single user interface offered with flexible deployment options Micro Focus’ OPTIC is a truly drama-free, next-generation IT platform. 📌

There's one thing even a
billion-dollar company can't afford:

a security breach

A person wearing a dark hoodie and gloves is holding a laptop in front of their face, obscuring it. They are standing in a dark, industrial-looking space with concrete pillars and windows in the background. The lighting is dim, with light coming from the windows, creating a moody and mysterious atmosphere.

Safeguard your IT
with
ManageEngine

Security Information & Event Management | Identity & Access Management
Network Security Management | Unified Endpoint Security & Management
Privileged Identity Management | Firewall Security Audit & Log Management

www.manageengine.com

Maheer Jadallah
Senior Director -
Middle East &
North Africa, Tenable



ANATOMY OF AN OT ATTACK

MAHER JADALLAH, SENIOR DIRECTOR - MIDDLE EAST & NORTH AFRICA AT TENABLE, DISCUSSES HOW, INSTEAD OF DEFENDING AGAINST AN ATTACK IN PROGRESS, A MORE SUSTAINABLE APPROACH WOULD BE ONE OF PREVENTION – OF ORGANISATIONS DOING A BETTER JOB OF UNDERSTANDING THEIR SYSTEMS, WHERE AND HOW THOSE SYSTEMS MAY BE EXPOSED, AND PRIORITISING THE THINGS THEY NEED TO PROTECT THESE SYSTEMS.

What are the cyber threats organisations face currently?

Attackers thrive during times of uncertainty and the last year

has provided plenty for them to work with. The world has changed, perhaps forever, and the way we work has been overhauled. We've seen organisations move to accommodate remote working, some overnight, with many looking at what that means for the future. The issue is that, when introducing any new working practice — such as remote working, it is critical to do so securely. Organisations need to think through how this changes the threat landscape and introduce controls to limit and/or address this risk.

With the remote working “hybrid” model likely to continue, at least for the foreseeable, this shift to a remote, distributed workforce has led to a higher

volume of critical and confidential information being transmitted electronically. Security leaders must ensure that their strategies are in lockstep with business priorities and can effectively communicate the security programme to business asset owners.

Of course, it's not just data breaches that are a concern. This expanded infrastructure poses a larger target for attackers and we've seen a number of instances where IT systems have been compromised, allowing the bad guys to move laterally and affect operational technology (OT) systems that power our critical infrastructure. The most recent being Colonial Pipeline, which was hit with ransomware that began in the IT environment and, out of precaution, forced the operator to shut down operations.

Another threat vector comes in the form of supply chain attacks. When we think of the SolarWinds breach at the end of 2020, that affected organisations in MENA and globally, threat actors were looking for any entry point from which to cause disruption, steal information

and monetize their crimes. The reality is that most organisations struggle to understand the systems they have control over, let alone those of their supply chain.

Knowing which systems are critical to remain operational, where and how those systems are exposed, and prioritising the steps needed to protect those systems from attacks is critically important. It's imperative that both the public and private sectors recognise the increased threats they face and join forces to remediate the risk posed if we're to turn the tide back in the defenders favour.

Why are we seeing a rise in successful attacks against OT infrastructure?

Critical service providers are far more impacted than the average organisation if they need to take any systems, let alone all of them, offline for any period of time. Bad actors know this and are actively looking for ways to capitalise on this.

When we think back, even just a decade ago, the majority of industrial systems were completely disconnected to the outside world. Today, that is no longer true. In

search of efficiencies, we see autonomous networks, from just a few systems — such as thermostats to keep a room's temperature controlled, to completely automated power plants, production lines and other environments. These systems are often powered by IT systems — meaning an attack against the IT side of the house, can easily impact the OT side.

As infrastructure is modernised and upgraded, these new components have ethernet built in. Some may even come with Bluetooth or WiFi functionality.

While this is all progress, and some would argue in the right direction, from a security stance each offers another potential open window through which an assailant can climb.

Can you discuss the anatomy of an OT attack?

Threat actors predicate most attacks by targeting a particular device — such as a server, switch, programmable logic controller (PLC), etc. Finding a weak device in a network is reconnaissance's key goal for example, an unguarded device, a device that uses a default password or an exploitation based on an unpatched vulnerability.

Having gained a foothold, for an attack to proliferate to other infrastructure areas, attackers will next focus on Active Directory to escalate privileges. In addition, if Active Directory serves as the organisation's Identity Provider (IdP), a compromise of it could impact a single sign-on (SSO) solution, giving attackers even more access to additional accounts which a user might be configured with access to. Once attackers have achieved that they really do have the keys to the virtual kingdom.

The bad actors will then use the network to perform further reconnaissance, extend the attack to find additional devices that they can defeat or use to get to other, previously secured parts of the environment to deliver the

attack, all without detection. It is not uncommon that reconnaissance can take weeks — or months — and may take more time than the actual attack itself.

Decades of experience in IT security yields important lessons that can be applied to OT. For example, simple network tapping and "listening" does not catch all attacks. Driving deeper to the device level, the target of most attacks, is a key method of early detection before an attack starts to propagate and find new targets to conquer. This is particularly relevant in OT environments where up to 30% of OT assets are dormant; meaning, they never communicate over the network. In these situations, network or passive-only detection would never catch a dormant infected device.

How can organisations better protect themselves and their OT environments?

Cyberattacks are a real and present danger, particularly when it comes to critical infrastructure, and by extension to every single consumer. Rather than try and defend against an attack in progress, a more sustainable approach is one of prevention — of organisations doing a better job of understanding the systems they have, where and how those systems may be exposed, and then prioritising the things

THE CHALLENGE IS THAT THE TOOLS AND PROCESSES OF YESTERDAY ARE BEING USED TO SOLVE TODAY'S PROBLEMS-BUILT & DESIGNED FOR THE OLD ERA OF IT...."

they need to do to protect those systems from attacks, including ransomware.

The challenge is that the tools and processes of yesterday are being used to solve today's problems — built and designed for the old era of IT when the attack surface was a static laptop, desktop or on-premises server. As a result, organisations struggle at every step — seeing their assets, detecting weaknesses, and prioritising issues for remediation.

Instead, organizations need a modern, comprehensive strategy to quickly and accurately identify vulnerabilities and misconfigurations in their dynamic infrastructures, that delivers clear guidance and recommendations on how to prioritize and remediate any risks.

This requires visibility across the entire infrastructure — it's not about IT, and it's not about OT, it's about the risk posed to the organisation, regardless of where





the attack originates and which systems could potentially be affected.

Attack vectoring takes the network and devices, whether IT, IoT or OT, into account. It redefines how to address attacks by identifying the high-risk pathways an attack may take if it were introduced to the environment. Running simulations can best determine weak points and where security interventions are needed before an attack launches.

In this manner, attack vectors group devices that share a backplane, such as PLCs, comm. adapters, I/O cards] to calculate any impact risk. Mapping pathways illustrate instances where reducing or eliminating risk closer to the demarcation point may reduce risk further down the line and deeper into the network. This helps zero-in on particular devices, sectors or locations in the environment that require special attention or interventions.

Having focused effort on what matters most, the next step is to identify and address vulnerabilities that attackers target.

Given that attackers look for vulnerabilities to exploit, closing off these flaws would thwart most attacks. However, each day a fresh stream of vulnerabilities are discovered that could put the organisation at risk. According to the National Vulnerability Database (NVD), over 18,000 vulnerabilities were disclosed in 2020. Yet, only 3% of vulnerabilities have a high probability of being leveraged in an attack. Even fewer were actually leveraged by attackers- meaning the vast majority of these vulnerabilities posed only a theoretical risk. For the average security professional, prioritising which of these vulnerabilities warrants attention is more challenging than ever, and not all vulnerabilities are created equal.

Other factors must be considered when weighing the severity of a vulnerability, including the presence of proof-of-concept (PoC) exploit code and ease of exploitation, helping organisations understand which flaws represent the greatest risk.

Improving Active Directory security is the next critical step in Risk-based Vulnerability Management. However, when it comes to Active Directory, most organisations struggle due to years of configuration mistakes and improperly defined access and user groups, hordes of inactive accounts and overly permissive settings. Organisations must take the time to audit their AD environment and develop best practices aligned to the organisation's unique needs to help reduce this risk. While there's no guarantee that a user with administrator privileges will not click on a link in a phishing email, reducing the number of users with inappropriate levels of access helps minimise an organisation's risk.

By empowering organisations to prioritise their vulnerability management results based on the privileges afforded to each end-user in the system, effectively disrupts the attack paths hackers use to install malware, move laterally and exfiltrate data. The security community is recognising the risk posed from threat actors, and responding by shifting the operating paradigm away from intrusion detection to one of prevention — or simply thwarting an attack before it can start. Gaining deep situational awareness about each and every device in the environment, identifying communication paths, access information and more, can help highlight weak spots and potential embarkation points for new attacks. It further empowers the security community to reduce risk and cyber exposure. This will strengthen the cyber security profile, rather than dealing with an incident after the fact. 🔒



COPING WITH THE NEW NORMAL

HUSNI HAMMOUD, MANAGING DIRECTOR - ESET ME, BARRACUDA NETWORKS, IVANTI (PART OF MIDIS GROUP), TELLS SECURITY ADVISOR HOW THE CHALLENGES OF THE LAST ONE YEAR HAVE CHANGED THE BUSINESS LANDSCAPE AND HOW ORGANISATIONS ARE NAVIGATING NEW TRENDS.

How would you describe the cybersecurity landscape in the region today, with so many changes having taken place since last year?

The pandemic that hit us last year changed the way we live, work and engage. The shift from the physical world to the virtual world opened up new opportunities for cyber criminals and they welcomed this with open arms, resulting in a barrage of COVID-19 themed attacks that put large segments of the economy at risk.

Things are much better now and the world has been able to adjust to the new normal but cybersecurity risks are still high, even though a large part of the industry has tried to plug the gaps that came into play because of the sudden shift of workforce from offices to homes, exposing both end-points and networks at risks. The uptake in adoption of cloud also created its own set of challenges for the cybersecurity industry.

The cybersecurity landscape never remains the same and it keeps on evolving with every single incident. The region has been known for political uncertainties for a long time now, and they also contribute in a big way in shaping this landscape.

If we look at several independent reports and data, one can easily say that cyber-attacks have grown in past one year and that the trend will continue in days to come.

How have the security priorities of organisations in the region changed since the pandemic?

The new normal has set new rules of engagement, and all organisations across the world have had to reassess

WE ARE CLOSELY ENGAGED WITH OUR PARTNERS, SUPPORTING THEM BOTH TECHNICALLY & FINANCIALLY, WHICH IS ESSENTIAL TO SUSTAIN THEIR BUSINESS."

and adjust their priorities accordingly. They were forced to evaluate new models that can work well with the rapid transition to remote working. Many companies have had to transition from the firewall approach of the traditional office to a new distributed model. Several organisations have to adopt cloud during the past year and now they are exposed to the challenges in the new environment.

How has your company, in particular, adapted to the changing business landscape? What challenges have you faced in the last one year or so?

We had a major test of our agility and resiliency during the last year. We had to make sure that we were operational and able to support our partners and customers in the region without any interruptions. We were able to apply our in-house tools and processes that managed Work from Home (WFH) and remote operations and support for the internal team and our customers. We also provided assistance to our customers during the critical pandemic and lockdown period for their infrastructure changes, upgrades and transition to the new

working model, with high availability and security.

It was a great lesson/challenge that we were able to share our internal experience with our channels and customers to minimise their business interruption, leveraging our existing acquired tools and support that we provided at the right time.

How are you collaborating with your partner network, to tackle these challenges?

We are closely engaged with our partners, supporting them both technically and financially, which is essential to sustain their business. As we all have witnessed, COVID-19 changed the requirements of customers virtually overnight, forcing them to focus on "must have" solutions from "good-to-have" technologies. In this scenario, we aligned with partners and helped them to adjust to the new realities and updated their product portfolio & service offerings, so that they can continue to support their customers and look for new opportunities in accordance with the situation.

Finally, what is your outlook for the cybersecurity market for the next few years, with the pandemic still unabated and impacting some of the key markets?

The market for cybersecurity will continue to grow in the coming years, as there is no relief on the cyber-attack front. New technologies will have their own security challenges, as we have already seen several incidents of vulnerabilities and risks associated with IoT devices. With the demand for cloud and 5G on upward trend, the demand to secure them will also stay strong. 📌

KASPERSKY SHEDS LIGHT ON THE RANSOMWARE ECOSYSTEM



Ransomware is on the tip of everyone's tongue every time businesses discuss cyberthreats they are likely to face in 2021. Attackers have built their brands and are bold in their advances like never before, with the news about organisations being

hit with ransomware consistently on newspaper front pages. But by placing themselves under the spotlight, such groups hide the actual complexity of the ransomware ecosystem. To help organisations understand how the ransomware ecosystem operates and how to fight it, the latest

report by Kaspersky researchers dug into darknet forums, took a deep look at REvil and Babuk gangs and beyond and debunked some of the myths about ransomware. And when you dig into this underworld, you have to expect that it has many faces.

Like any industry, the ransomware

ecosystem comprises several players that take on various roles. Contrary to the belief that ransomware gang are actually gangs – tight, have been through it all together, Godfather-style groups, the reality is more akin to the world of Guy Ritchie's 'The Gentlemen', with a significant number of different actors – developers, botmasters, access sellers, ransomware operators – involved in most attacks, supplying services to each other through dark web marketplaces.

These actors meet on specialised darknet forums where one can find regularly updated ads offering services and partnerships. Prominent big-game players that operate on their own do not frequent such sites, however, well-known groups such as REvil that have increasingly targeted organizations in the past few quarters, publicize their offers and news on a regular basis using affiliate programs. This type of involvement presumes a partnership between the ransomware group operator and the affiliate with the ransomware operator taking a profit share ranging from 20-40%, while the remaining 60-80% stays with the affiliate.

Selection of such partners is a finely-tuned process with ground rules set by the ransomware operators from the start – including geographical restrictions and even political views. At the same time, ransomware victims are selected opportunistically.

As the people who infect organisations and the ones who actually operate ransomware are different groups, only formed by the desire to profit, the organisations infected most are often low hanging fruit – essentially, the ones that the attackers were able to gain easier access to. It could be both actors that work within the affiliate programs and independent operators that later sell access – in an auction form or as a fix, starting as low as 50 USD. These attackers, more often than not, are botnet owners who work on massive and



wide-reaching campaigns and sell access to the victim machines in bulk, and access sellers on the lookout for publicly disclosed vulnerabilities in internet facing software, such as VPN appliances or email gateways, which they can use to infiltrate organisations.

Ransomware forums are home to other types of offers too. Some ransomware operators sell malware samples and ransomware builders for anything from 300 to 4,000 USD, others offer Ransomware-as-a-Service – the sale of ransomware with continued support from its developers, which can range from 120 USD per month to 1,900 USD per year packages.

"In the past two years, we have seen how cybercriminals have become bolder in using ransomware. Organisations targeted by such attacks are not limited to corporations and governmental organisations – ransomware operators are ready to hit essentially any business regardless of size. It is clear that the ransomware industry per se is a complex one involving many different actors with various roles. To fight them, we need to

educate ourselves on how they work and fight them as one. Anti-Ransomware Day is a good opportunity to highlight this need and remind the public of how important it is to adopt effective security practices. INTERPOL's Global Cybercrime Programme, together with our partners, is determined to reduce the global impact of ransomware and protect communities from harm caused by this growing threat," comments Craig Jones, Director of Cybercrime, INTERPOL.

"The ransomware ecosystem is a complex one with many interests at stake. It is a fluid market with many players, some quite opportunistic, some – very professional and advanced. They do not pick specific targets, they may go after any organisation – an enterprise or a small business, as long as they can gain access to them. Moreover, their business is flourishing, it is not going away anytime soon," comments Dmitry Galov, security researcher at Kaspersky's Global Research and Analysis Team. "The good news is that even rather simple security measures can drive the attackers away from organisations, so standard practices such as regular software updates and isolated backups do help and there is much more that organisations can do to secure themselves'.

"Effective actions against the ransomware ecosystem can only be decided once its underpinnings are truly understood. With this report, we hope to shine a light on the way ransomware attacks are truly organised, so that the community can set up adequate countermeasures," adds Ivan Kwiatkowski, senior security researcher at Kaspersky's Global Research and Analysis Team. 📌

SOME RANSOMWARE OPERATORS SELL MALWARE SAMPLES AND RANSOMWARE BUILDERS FOR ANYTHING FROM \$300-4,000, OTHERS OFFER RANSOMWARE-AS-A-SERVICE."

REINFORCING A COLLABORATIVE APPROACH TO CYBERSECURITY

IN AN EXCLUSIVE INTERVIEW WITH ANITA JOSEPH, EDITOR, MIKA LAUHDE, VICE PRESIDENT OF CYBERSECURITY & PRIVACY – GLOBAL PACD, HUAWEI, DISCUSSES HOW HUAWEI WORKS TOGETHER WITH CUSTOMERS, PARTNERS AND OTHER INDUSTRY PLAYERS IN THE REGION TO ELEVATE ITS ICT INDUSTRY TO THE NEXT LEVEL.

What are some of the key cybersecurity threats facing the region today?

The global challenges we faced as a society last year led to fundamental changes in our physical and digital environments. This caused countries to prioritize resolving internal matters first, and global collaboration against cyberthreats wasn't given its due attention. This lack of global collaboration has impacted our cybersecurity landscape. Cybercriminals, on the other hand, have become very sophisticated and organised, leveraging cross-border networks to exploit vulnerabilities across the globe.

During this time, we also witnessed a rise in remote working, and this presented unique challenges from a cybersecurity perspective. Work devices no longer operated on an organisation's secured perimeter. Devices that connected to corporate networks through unsecured connections led to vulnerabilities that could be easily exploited by nefarious

threat actors. Furthermore, IoT and webcams were exploited, with instances of virtual conference hacking (called Zoom bombing) leading news agendas. Cybersecurity teams had to spring into action to serve a dual purpose of ensuring business continuity, and protecting its enterprise network.

Despite this sensitive global situation, some state actors used this opportunity to interfere with national security and stability. Some of the common threats we faced were disinformation and phishing. Disinformation was prevalent throughout 2020 because of the pandemic where people obtained news from unofficial sources and, therefore, causing chaos and confusion. In addition, hackers made use of the situation and sent phishing emails masquerading as official authorities on national initiatives, such as financial aid, where the targets were directed to the hacker's site to collect their personal data. This led to a third threat which was online identity theft and stealing individuals' money.

Can you share with us some of the best practices that organizations must follow, in order to address these challenges?

Humans can be the weakest and strongest link in a cybersecurity landscape. Besides technical adaptations for this new normal, it is now more important than ever that companies build holistic safety and security knowledge among employees to protect both corporate and personal data. This is the key organization's cyber assurance.

Organisations also need to provide new technical tools that allow secured connections while working from homes. This needs to be backed up with an upgraded cybersecurity strategy and policies. For multinational organisations, it is imperative that they quickly agree on global policies, keeping in mind the national regulations and differences.

We suggest the adoption of a common, baseline cyber hygiene, which goes back to the fundamentals as guidance for WFH. This is applicable for Small and Medium Sized Enterprises (SMEs) as well.

1) Adopting a strong password policy

- a. Eight or more characters
- b. Alpha numeric characters
- c. Mixture of upper- and lower-case characters
- d. Special characters

2) Making use of multi-factor authentication for identity management

- a. For key services, make use of non-SMS 2nd factor authentication
- b. VPN

3) Must have a computer usage policy, no matter how simple it is

4) Keeping your OS and software updated

- a. Enable auto-update where possible

5) Make use of SaaS services whenever possible (a cloud-first strategy is recommended)

- a. While it is a shared responsibility model for cloud, in a SaaS environment, the provider is responsible for most of them.

Biometrics and contactless technologies



are beginning to play a major role in the market today. What are some of the trends and emerging opportunities in this area?

Biometrics and contactless technologies are spreading globally, especially that the COVID-19 pandemic has brought these technologies into greater focus as a sustainable approach for contactless authentication.

In the UAE, for example, the country has been accelerating the usage of biometrics and contactless technologies due to COVID-19. Contactless menus and payment systems in restaurants and shops is now a commonality that most will consider that as a basic service. Biometrics are also used in border controls at airports. The UAE has launched facial recognition and Iris recognition, replacing traditional fingerprint authentication.

I would expect the proliferation of non-invasive technologies in the area of biometrics and contactless to continue, building on the momentum brought about due to the pandemic. Tighter integration with AI at the backend would be required to deliver more innovative solutions to the customers

That said, there might still be security concerns from privacy systems and issues surrounding personal data rights. We at Huawei believe these should not be overlooked, and are committed to creating safe, transparent, and cooperative cyber cybersecurity mitigation programs to ensure we protect any sensitive information.

How would you assess the progress made by the Middle East region, particularly the UAE, with regard to cybersecurity regulations and technology adoption?

The UAE is well poised to become one of the globally trusted hubs, with strong foundations in place like the UAE Cybersecurity Strategy since 2019. Furthermore, the establishment of the UAE Cybersecurity Council, and the appointment of H.E. Dr. Mohamed Al Kuwaiti as its chair and the CSO of the UAE government, provided the right foundation for the UAE to build up its cybersecurity credentials.

The UAE government correctly made the decision that all technology advancement brought about by Industry 4.0 and deep tech should be deployed with the right strategy, taking the security and privacy-by-design

approach, baking these rights into their solutions from day one.

Please tell us about Huawei's work in the region, as far as cybersecurity and technology are concerned.

Huawei is a global leader in the ICT field. With that, we recognise that we need to adopt an open, transparent, and collaborative approach in working with all the stakeholders in the ICT ecosystem. Through inclusive industry development where we work together with our customers, partners, standards organisations, and all other industry players in the Middle East region, we are able to elevate the entire Middle East ICT industry to the next level. This sharing and collaboration will enable all of us within the ICT community to develop new innovative products, services and capabilities.

Across the Middle East, Huawei is working conscientiously to promote security by offering products that are developed using security-by-design principles, and delivering solutions based on a zero-trust approach. We work closely with local leaders and stakeholders, including institutes of higher learning, in an effort to support capacity building in cybersecurity across all our markets in this region. As a part of our contribution to local talent development, Huawei has committed to training around 10,000 professionals in the UAE in the next three years, helping them to be future-ready.

Huawei solutions for enterprises, such as Huawei Cloud, are designed with security in mind. It has all the necessary cybersecurity and privacy protection international certifications such as ISO 27001, ISO 27017, ISO 27018, CSA STAR Gold, AICPA SOC and PCI DSS globally. Our UAE cloud infrastructure, which we built and hosted locally, is also constructed using these industry-leading solutions.

By combining cybersecurity, privacy and data protection, risk, governance and compliance, resiliency, and business continuity together, we wish to be a catalyst for the local ICT ecosystem's success. 🙌

ENSURING A SAFE & SECURE DIGITAL TRANSFORMATION FOR TODAY'S COMPANIES

BY JIHAD TAYARA, CEO OF EVOTEQ



Digital transformation has become a top-of-the-mind initiative for many of today's companies and organisations. Although initiatives like these may result in positive impacts, newer issues can also emerge, citing the absence of an effective and sustainable cyber risk program.

Currently, the Middle East is addressing what experts call a cyber pandemic, wherein COVID-19 related attacks have seen a dramatic increase in numbers. Rapid digitalisation, which is now being witnessed in countries such as the Kingdom of Saudi Arabia (KSA) and the United Arab Emirates (UAE), has prompted the usage of smart connected devices, thus opening possible gateways for cyberattacks.

The coronavirus (COVID-19) outbreak has changed the way we do things. One such change can be seen in the current state of business resiliency and productivity demands. The digitalised processes — roughly translated — would mean that greater volumes of sensitive data is now being shared and facilitated through email and file transfers, which increases the risk of data leakage.

Owing to the technological advancements across a highly competitive landscape, businesses have to deal with pressures of a rapidly evolving business scene and forever changing market demands. Not being able to keep up with the pace of innovation may put businesses at risk across today's marketplaces.

As these transformations pick up momentum, businesses are increasingly under risk from attacks on digital technologies. In such a scenario, staying secure is not an easy task to maintain. Industry experts recommend integrating cybersecurity measures into the overall digital business strategy—a move to further realise the benefits of digital transformation.

The advent of these newer technologies has prompted what experts call a 'digital transformation entrepreneurial journey'. Security should be viewed as a key part of digital enterprises and built into the core of the business, which in turn, will help ensure a dependable and reliable framework needed to achieve a secure digital transformation. Because of possible security risks that come with these new digital processes, securing investments becomes harder as stakeholders cannot tolerate the effects brought about by digital change.

The regional governments are highly aware of the importance of this shift. In fact, these economies are now improving their cybersecurity systems by increasing protection levels of their critical national information infrastructures. Leading experts suggest companies to integrate security and risk governance into the digital foundation of their organisations.

Further, the creation of a national cybersecurity program will both seek participation of the public and the private sector, leading to a secure and established IT framework to build a solid foundation for a

healthy data security plan. At the same time, investments should be made into equipment and processes, which can ultimately result in safe working environments.

The most significant aspect lies in the implementation of these new technologies by companies and organisations, which can lead to a protected and secure journey of digital transformation enterprises. It is also crucial to consider how the respective programs of these enterprises help in educating employees to make them aware of the importance of data security.

In line with these digital transformational changes, it is best to comply with the latest globally accepted standards in data privacy, which means there would also be a need to adopt new organisational culture and practices. With this in mind, both the customer and their data should be integrated into the company's privacy strategy.

Data processes, along with definition of roles and procedures, need to be created to address these changes. Companies should be prepared to respond to these cyberattacks and have solutions like recommended privacy programs in place to gain customer loyalty and help bring value to the brand itself. It is always best to remember that security is holistic and should be more of a separate entity in the process of digital transformation. We may be investing in the equipment, systems, and the like, but nothing will work or be as effective unless people are trained and made aware of the significance of digital transformation security. 🙌

LEADING THE CYBERSECURITY MARKET THROUGH INNOVATION

DEMES STROUTHOS, GENERAL MANAGER - ESET MIDDLE EAST, TELLS SECURITY ADVISOR THAT ESET IS COMMITTED TO KEEPING UP WITH INDUSTRY STANDARDS & GUIDELINES AND STRIVES TO CONTINUALLY DEVELOP AND INNOVATE ITS CYBER SECURITY SOLUTIONS.



How have the challenges of the last one year or so, affected the cybersecurity landscape?

Clearly, the year 2020 was quite challenging for organisations and individuals in terms of cybersecurity, along with the adoption of new working habits, especially since the COVID-19 outbreak in March 2020. The ESET Q4 2020 Threat Report reveals that the new attack surface created by the shift to work from home brought on further growth of Remote Desktop Protocol (RDP) attacks. Between Q1 and Q4 2020, ESET telemetry recorded a staggering 768% increase in RDP attack attempts. Another trend observed in Q4 was an increase in email phishing attacks. Organisations must secure their newly implemented remote working practices and maximise their ability to prevent, detect and respond to threats.

With cloud gaining traction, how is ESET helping companies secure their digital/cloud assets? In particular, what are some of the latest products and services that you offer in this area?

With digital transformation and new

market realities like remote workforce, there is an increased focus on Zero Trust Security, Gartner's CARTA to protect enterprises from cyber threats. ESET is committed to keeping up with industry standards & guidelines and strives to continually develop and innovate our cyber security solutions.

Earlier this year, ESET launched ESET Protect Cloud for real-time, continuous visibility across the endpoints whether they are inside or outside the enterprise network. ESET Cloud Office Security (ECOS), one of the recent releases, is a new Security-as-a-Service offering powered by machine learning and real-time cloud-based threat intelligence to enhance protection for Microsoft 365 applications. Another recent release is ESET Cloud MDM to protect the company's android devices from malware and enable MDM functionality on android & iOS platforms. Needless to say, ESET's Multi factor Authentication (MFA), Cloud Sandbox subscription, Endpoint Detection & Response (EDR) addresses the current security challenges for businesses implementing a 'cloud-first' strategy for their IT security.

How do ESET's products & solutions give businesses a greater technical edge?

What is the USP of ESET's products in a market that is full of competitors?

We have been developing cybersecurity solutions for more than 30 years now. ESET helps businesses adopt a holistic security approach by offering complete prevention, detection, and response capabilities to cyber threats with real-time, continuous visibility and monitoring of threats and endpoints from a single pane of glass. ESET solutions are recognised in the industry and regularly acknowledged by leading analysts and independent testing organisations. Almost 40% of ESET's employees work in R&D and actively contribute to the MITRE ATT&CK knowledge base. ESET solutions have been commended by analyst firms for its multiple, advanced ML algorithms for discovering malicious activity patterns. ESET solutions are well balanced in terms of speed, detection, and usability. ESET protects over 110 million users in 200 countries & territories globally which gives us wide coverage on emerging threats. 🛡️

OVERCOMING THE CYBER-PANDEMIC

ABHIJIT MAHADIK, DIRECTOR, CYBERSECURITY & INFRASTRUCTURE – UAE & KSA, RAQMIYAT SPEAKS TO SAME ABOUT THE EVOLVING CYBERSECURITY LANDSCAPE, THE THREATS ORGANISATIONS NEED TO WATCH OUT FOR AND HOW THE SECURITY PRIORITIES OF ORGANISATIONS HAVE SHIFTED SINCE THE PANDEMIC LAST YEAR.

At the outset, let me share with you a statement that clouds my mind. Isn't the cybersecurity market overcrowded already? Yet there is an ever-increasing influx! This brings me to another question: If so, then why are perpetrators always ahead of the game?

'Attacks against remote access protocols in the UAE reached 15.8 million in 2020,' according to a report by global cybersecurity company, Kaspersky.

Let me give you another outlook- today, 90% of cybersecurity professionals in the US and Japan anticipate malicious AI-powered attacks. This is because AI research is publicly available and it can be used to build intelligent, continuously learning exploits by attackers. In adversarial attacks, attackers even change the inputs of machine learning models to cause the model to make mistakes. Even if we all tend to agree that it's not a human scale problem anymore, how may we box the billions of data bits and time-varying signals sent from all corners? While new layers and surfaces both horizontally and vertically keep getting added to the organisation's

tech processes, a recent survey showed that while 85% of CISO's prime objective is protection from 'unknown' adversarial attacks, 76% are also wary of regulatory non-conformities, 72% are grappling with cybercrimes and frauds too.

Tell us about the cyberattack landscape in the Middle East right now. What should we be worried about?

The Middle East region is facing a "cyber pandemic" as hackers take advantage of the Covid-related digital adoption, with a 250% increase in cyberattacks this year, and phishing and ransomware incidents increasing in frequency and becoming a soft target of "huge attacks," according to the head of the UAE Government's Cyber Security division.

However, to look at the sunny side of things, the Middle East is on a perfect journey of digitisation and complete

transformation programs have been rolled out to bolster capabilities across infra, telco, banking, energy, utilities, government as well as the entertainment sectors. Initiatives such as the KSA Transformational Program as well as Dubai's aim to become the best place to live by 2030 provides ample proof that it is truly a national drive.

On the other hand, Middle East governments are acutely aware of the new threat landscape associated with digitisation. In fact, to bolster their national cyber-security capabilities and elevate the protection level of their critical national information infrastructures, many of them have stepped up their cyber-security activities in recent years. Also, organisations in the region are facing more stringent regulations, forcing them to take greater responsibility for the protection of sensitive data. In short, it has become clear that security must keep pace with the speed of national initiatives.

What are some of the less common but extremely dangerous cyber-attacks that enterprises must be aware of? What can they do to prevent this?

Public Infrastructure Systems and Government IT systems have become a target of choice for hackers globally. As in the news, malicious actors, backdoors, commodity ransoms, etc are all knocking government agencies and financial institutions across. Newer APT groups are targeting the airline and hotel sectors in the wake of the Covid-19 pandemic. It won't be out of place to say that we are in the middle of a "Cyber Pandemic," too.

THE MIDDLE EAST REGION IS FACING A CYBER PANDEMIC AS HACKERS TAKE ADVANTAGE OF THE COVID-RELATED DIGITAL ADOPTION."

What are some of the less common but extremely dangerous cyber-attacks that enterprises must be aware of? What can they do to prevent this?

NotPetya Smaller footprints but bigger damage than Wannacry – Costliest attack globally but not heard of much in the Middle East today.

StuxNet which has rocked governments-a complex, multifaceted malware that can reprogram controllers at nuclear reactors.

Mirai another one that is termed as a giant botnet for large scale DDOS and has also been known to infect Playstations at large.

These are the less common but more dangerous ones. To begin with, a Cyber Resilience Check-up is the key to understand to what extent your defences are adequate. There is also a need to strengthen supply chain resilience capabilities, as that is one of the most vulnerable spots where most of the attacks have increased beyond control.

How have the security priorities of organisations shifted post the Covid-19 pandemic?

The shift in roles and responsibilities for the protection of sensitive data can be seen in the kind of initiatives taken up regarding data classification, the protection of crown jewels. There is also significant emphasis on business continuity planning in automation and sustenance in the wake of attacks and non-conformities found. Continuous Compliance Monitoring has also been embraced by telecom giants in the region.

In the context of shifting priorities and evolving cyberattacks, how do AI and machine learning step in, to accelerate enterprise security?

AI and Machine learning have been instrumental to some extent in alleviating

'alert fatigue' and 'false positives', recognising patterns and managing accurate response and threats before a disaster occurs, that too without the need for human intervention. However, the perpetrators bring in a far more focused AI and ML-based attack vector array. Here, contextualisation and prioritisation are key. Therefore, cybersecurity needs to be a board-room focus area to bring in the right business context-based cyber resilience into play.

What is your advice to organisations looking to strengthen their cybersecurity infrastructure?

There are some key aspects here: the first would be to bring in real-time visibility of business exposure due to cyber risks. The other factors would be

to draw a correlation between the

ROI of cyber investments

and losses owing to

cybersecurity, detect

and eliminate

overlapping security

technologies and

bring in near

real-time visibility

and transparency

on business

exposure. 🗝️



ALL ABOUT CYBERCRIME



Maher Jadallah
Senior Director -
Middle East & North
Africa, Tenable

The COVID-19 pandemic, which brought about a significant spike in demand for cloud adoption and remote working technologies, caught CISOs across the world off-guard, with many of them scrambling to find solutions to best protect their critical infrastructure and ensure business continuity. With the theme 'Enabling Resilience in Digital Economies,' GISEC's conferences will welcome innovators, CISOs, CIOs, CTOs, regulators and policymakers across government, finance, healthcare, telecom, energy and utilities, among others, to unravel strategies to form

It's finally happening: GISEC, the region's largest and most impactful cybersecurity expo and conference, is taking place live and in-person here, in the vibrant, thriving city of Dubai. With a focus on combating rising incidents of cybercrime, this exciting platform

brings together decision-makers, cybersecurity experts and technology professionals to discuss and debate the latest breakthroughs and innovations in Artificial Intelligence (AI), IT, 5G and the cloud, impacting the cybersecurity posture across organisations.



Ned Baltagi
Managing Director Middle
East and Africa, SANS
Institute

a strong and resilient cybersecurity ecosystem that inspires trust and confidence in the digital economy. Debut pavilions from countries such as Germany and Turkey will be one of the many highlights of the show.

Some of the participants at this year's event are all set to show case cutting-edge products and solutions that promise to stay ahead of the attackers. For instance, Tenable, the cyber exposure company, will highlight its Active Directory Security capabilities. "The acceleration of digital transformation and remote work models over the past year has resulted in a surge of cybercrime. Active Directory is a prominent and valuable target for threat actors who can use to gain access into a network and conduct further attacks," said Maher Jadallah, regional director - Middle East, at Tenable. "At GISEC 2021, we look forward to having impactful conversations and discussing the most effective ways for customers to see, predict and reduce cyber risk in the digital era."

With a strong commitment to promoting cyber resilience and empowering organisations to deal with security challenges in the post-pandemic new normal, SANS institute has confirmed that it will be the Official Training Partner for GISEC and bring several new products like Cyber Ranges, SANS Foundations and CyberStart to the event. SANS will also display its latest range of world-leading training courses and certifications that promote cyber resilience and empower organisations to deal with security challenges in the post-pandemic new normal. "The pandemic has forced organisations to accelerate their digital transformation initiatives, which has put them at risk in new and unprecedented ways. Cybersecurity is now front and centre

of these initiatives. However, the gap for cybersecurity jobs is widening and organisations need to act now to equip and train their staff with skills to deliver best-in-class defence. At GISEC 2021, we plan to highlight this message and demonstrate how our programs can help organisations arm themselves against potential cyber-attacks and narrow the cybersecurity skills gap," said Ned Baltagi, Managing Director Middle East and Africa at SANS Institute.

GISEC 2021 will also train the spotlight on countries such as Saudi Arabia and South Africa, to examine the impact of cybercrime in these key markets and the increased demand for more comprehensive, up-to-date technologies and advanced cybersecurity solutions. There will also be a special conference dedicated to the role of women in the global cybersecurity arena. In fact, studies show that only 20% of the global cybersecurity workforce and 5% of the Middle East workforce are currently women. The conference will bring together global cybersecurity players and decision-makers to revisit and revise policies so that more women can be encouraged to become part of the industry.

This year's event, which brings a sense of normalcy and "connectedness" to the events space, is eagerly anticipated for its bold and innovative approach to one of the biggest, but most overlooked aspects of business success. It is being hailed for its unified, collaborative approach to the battle against cybercrime and the increasingly complicated threat landscape. One of the most defining cybersecurity events in the regional events map, GISEC 2021 is a must-visit for everyone interested in futuristic defence tactics and technology-enabled cyber protection. See you there! 📍



Spire Solutions

Mohieddin Kharnoub
Chief Revenue Officer,
Spire Solutions

What does participation in GISEC mean this year, particularly after a hugely challenging 2020?

We believe that the pandemic has brought about many critical cybersecurity challenges to governments and enterprises, which can be resolved through collaborative efforts. At Spire Solutions, we took the initiative of introducing Business Integrated Cyber Security Solutions that offer better visibility and help our customers with remediation against threats targeting their digital assets. Also, as businesses have started getting distributed everywhere, it becomes important to secure everything - Data, People and Devices - so we are prioritising those aspects. At GISEC, we will be demonstrating several of our niche cyber security solutions that make continuous security happen and also highlight our big data offerings.

What, in your opinion, should be the key cybersecurity priorities for organisations in the region today?

While cyber security is becoming broader and deeper, some of the current key priorities in my opinion, centre around visibility, digital risk management, Artificial Intelligence (AI) & Machine Learning (ML) empowered security, security orchestration and automation for effective incident response, threat hunting and intelligence, cloud security, big data for security analytics, IoT security, human risk management via security awareness and continuous security validation.

FORTINET: MAKING A MARK @ GISEC

ALAIN PENEL, REGIONAL VICE-PRESIDENT, MIDDLE EAST & PAKISTAN AT FORTINET, EXPLAINS WHAT IT MEANS TO BE A PART OF GISEC THIS YEAR AND HOW FORTINET'S CUTTING-EDGE SOLUTIONS CONTINUE TO PROVIDE MAXIMUM PROTECTION AGAINST CYBERTHREATS AND ATTACKS.

What is Fortinet looking forward to at GISEC this year? Do you think the event will be different from the previous years?

Fortinet welcomes a great degree of normalcy to a key industry platform such as GISEC which gives us an opportunity to network and showcase our industry-leading solutions. The pandemic has demonstrated how important wise cybersecurity investments are to enabling business continuity. We are looking forward to engage with C-level decision makers to help them unravel complexities in their security investments and create effective security designs and strategies that work in today's threat landscape.

What will Fortinet's focus be at GISEC this year?

This year we will showcase one of our latest solutions which delivers advanced, real-time threat intelligence, visibility, analysis, management, and protection for endpoints both pre- and post-infection, FortiEDR. It proactively reduces the attack surface, prevents malware infection, detects and defuses potential threats in real time, and can automate response and remediation procedures with customizable playbooks. FortiEDR also eliminates alert fatigue and breach

anxiety, standardizes your incident response procedures, and optimises your security operation resources with advanced automation.

In addition, we will continue to emphasise our industry leading Fortinet Security Fabric. Flexible, adaptable, broad, intelligent and automated, its solutions are integrated into a unified, cohesive, and end to end security platform offering actionable threat intelligence and AI-based security automation tools. The Fortinet Security Fabric consolidates and accelerates networking and security through a security-driven networking approach to deliver full visibility and the highest scalability combined with advanced security to protect business-critical applications across distributed and hybrid ecosystems.

Finally, yet importantly, our Secure SD-WAN solution which provides all the networking and connectivity features of the most advanced SD-WAN solutions, but with a critical differentiator: it also includes a full stack of integrated, enterprise-class security features, and centralized management so it can be seamlessly incorporated into the larger corporate security framework.

By leveraging Secure SD-WAN, Security-Driven Networking, and an expansive security fabric to protect their WAN, Cloud,

and datacenter edges—where security and networking function as a single solution—organisations can be better prepared to face the security challenges presented by digital innovation while enabling reliable and self-healing networks.

How do you think the cybersecurity landscape has changed since the pandemic?

The last year has demonstrated an unprecedented cyber threat landscape where cyber adversaries maximised the constantly expanding attack surface to scale threat efforts around the world. The pandemic has played a central role, adversaries proved to be highly adaptable, creating waves of disruptive and sophisticated attacks. They have targeted the abundance of remote workers or learners outside the traditional network, but also showed renewed agility in attempts to target digital supply chains and even the core network.

The pandemic has also accelerated digital transformation, expanding perimeters and the number of network edges. Now those edges are multiplying, and we have to worry about not only the enterprise perimeter but our wide area network and the multiple clouds that we use. Cybercriminals are fully aware of these vulnerabilities, as well as the fact that for far too many organisations, a full security strategy often lags behind network expansion.

By monitoring the threat landscape, partnering with the right vendors, and establishing valuable alliances, organisations can better protect their employees while also helping the industry as a whole stay ahead of modern threats.

With digital transformation in fast-track mode, what are some of the emerging security threats, in your opinion?

The new distributed network, including the new home office and transformed branch office, has added layers of complexity for organisations. Overburdened security teams, stretched thin across the expanding attack surface and suffering from the cybersecurity skills gap, are often unable to keep up. Cybercriminals are all too ready and eager to target this new edge environment. Malware targeting endpoint devices will be used to detect and exploit edge networks. They will be used to collect information, spread malware, and create botnets.

What organizations need is a security-driven networking approach that combines networking and security into a holistic solution that can begin protecting any edge the moment it is created. Additionally, the speed at which malicious cyber events can occur will also require the inclusion of edge AI, or edge intelligence, so that organisations can fully unleash the potential of the edge while responding to threats in real time.

Tell us more about the Fortinet Security Fabric. How does it help enterprises stay ahead of the growing threat landscape?

The Fortinet Security Fabric is the industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich open ecosystem. It spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect devices, data, and applications.

The Fortinet Security Fabric supports more consumption models than any other solution, including physical, virtual, cloud,

**THIS YEAR, WE WILL
SHOWCASE ONE OF OUR
LATEST SOLUTIONS
WHICH DELIVERS
ADVANCED, REAL-TIME
THREAT INTELLIGENCE,
VISIBILITY, ANALYSIS,
MANAGEMENT AND
PROTECTION FOR
ENDPOINTS BOTH PRE-
AND POST INFECTION,
FORTIEDR.**

and as-a-Service environments. It encompasses the industry's broadest product portfolio, spanning network security, SD-WAN, switching and wireless access, network access control, authentication, public and private cloud security, endpoint security, and AI-driven advanced threat protection solutions – all built on a common operating system, FortiOS. 🦋



SANS INSTITUTE TO FOCUS ON CYBER RESILIENCE AND TRAINING AT GISEC 2021



Ned Baltagi
Managing Director Middle East and Africa,
SANS Institute

SANS Institute has confirmed that it will be the Official Training Partner for the Gulf Information Security Expo & Conference (GISEC), to be held at the Dubai World Trade Center from May 31 to June 2, 2021. GISEC has emerged as the Arab world's largest and most impactful cybersecurity event, and SANS Institute will bring several new products like Cyber Ranges, SANS Foundations and CyberStart to the event, and also display its latest range of world-leading training courses and certifications that promote cyber resilience and empower organisations to deal with security challenges in the post-pandemic new normal.

"The pandemic has forced organisations to accelerate their digital transformation initiatives, which has put them at risk in new and unprecedented ways. Cybersecurity is now front and center of these initiatives. However, the gap for cybersecurity jobs is widening and organizations need to act now to equip and train their staff with skills to deliver best-in-class defense. At GISEC 2021, we plan to highlight this message and demonstrate how our programs can help organizations arm themselves against potential cyber-attacks and narrow the cybersecurity skills gap," said Ned Baltagi, Managing Director Middle East and Africa, SANS Institute.

Cyber Ranges is a comprehensive suite of hands-on ranges that come with industry-leading interactive learning scenarios. SANS BootUp CTF, for example, is a collection of challenges that help beginners and intermediate players build fundamental hands-on skills in a wide set of cybersecurity disciplines; NetWars Tournaments & Continuous provides cutting-edge cyber challenges within an integrated storyline; and NetWars CyberCity is a kinetic cyber range for learning how to analyse and assess the security of control systems and related infrastructures, and find vulnerabilities that could result in significant kinetic impact.

Cyber42 Cybersecurity Leadership Simulation Games deliver the ultimate hands-on challenges for testing and building your cybersecurity management skills; Jupiter Rockets provides an in-depth

offensive simulation for pen testers and red teamers; while Cyber Situational Training eExercise (Cyber STX) is a premiere in-depth training and validation cyber range.

SANS Institute will also talk about SANS Foundations, which has been designed to impart core knowledge and develop practical skills in computers, technology, and security foundations. The course features a comprehensive variety of innovative, hands-on labs and practical exercises that go far beyond what is offered in any other foundational course in cybersecurity. The labs are developed by leading subject-matter experts, drawing on the latest technology, techniques, and concepts in cybersecurity.

CyberStart Game is an online gamified learning platform used in the classroom or accessed at home. It is available to students, teachers and young adults across the Middle East and Africa region. CyberStart Game is designed to teach complex security concepts, while promoting self-exploration and investigation over traditional learning methods. Participants can play over 200 challenges, and are in control of their learning as they train at pace that suits their ability.

SANS Institute has been working with government and commercial organisations in the region, helping upskill security professionals and introduce new talent into the cybersecurity industry. Visitors to GISEC 2021 can drop by at Booth C14 to interact with experts from SANS Institute. 



GISEC

GULF INFORMATION SECURITY EXPO & CONFERENCE
معرض ومؤتمر الخليج لأمن المعلومات

*Live,
in-person*

31 MAY -
2 JUNE 2021

DUBAI WORLD
TRADE CENTRE

THE MOST INFLUENTIAL AND CONNECTED

CYBERSECURITY EVENT FOR THE ARAB WORLD

ENQUIRE ABOUT EXHIBITING, SPEAKING AND SPONSORSHIP

☎ +971 (04) 308 6267

✉ gisec@dwtc.com

🌐 www.gisec.ae

OFFICIALLY SUPPORTED BY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER



OFFICIAL DISTRIBUTION PARTNER



STRATEGIC SPONSORS

vmware
Carbon Black



SILVER SPONSORS

BLUVECTOR
A COMCAST COMPANY



COUNTRY PAVILIONS





GAJSHIELD: ENABLING CONTEXTUAL VISIBILITY FOR OPTIMUM DATA PROTECTION

HARRISON ALBERT, REGIONAL DIRECTOR, D-LINK MIDDLE EAST AND AFRICA, TELLS SECURITY ADVISOR MIDDLE EAST HOW GAJSHIELD'S CONTEXT-BASED APPROACH TO SECURITY HELPS ORGANISATIONS FIND ANOMALIES, REDUCE FALSE ALARM AND PREVENT INTENTIONAL & UNINTENTIONAL DATA EXPLOITATION.

Security of cloud devices is a huge challenge. In this context, how do you ensure the security of your cloud product and service offerings?

GajShield's cloud product and services are protected using multiple layers of security. Data security is at the core of GajShield's business. We take personal data protection seriously with highest privacy and security standards. GajShield processes only limited amount of personal data with the consent of its customers, all of which is encrypted or anonymised. GajShield uses its own state-of-the-art operational security technology like Intrusion Prevention System, Insider risk protection and secure access to its infrastructure through multi factor authentication with safe credentials. GajShield's infrastructure is hardened against DDOS attacks and traffic is monitored round the clock. GajShield's data centers are configured with fail-over capabilities ensuring availability and resilience of its services in case of technical incidents.

Gajshield is at the front of security, especially data security. Tell us more about the company's data leak prevention solutions.

The Data Leak Prevention Solution is an integral part of our Data Security Firewall and acts as a core solution that helps prevent data leak through various platforms. It identifies, monitors, logs and prevents misuse and exploitation of the data when transferred from a network through deep content inspection and a contextual security analysis of transactions, DLP systems act as enforcers of data security policies.

They provide a centralised management framework designed to detect and prevent the unauthorised use and transmission of your confidential information. DLP protects against mistakes that lead to data leaks and

“GAJSHIELD E-MAIL SECURITY ENABLES ENTERPRISE USERS TO COMMUNICATE SECURELY & PROTECTS THEM FROM THE LATEST E-MAIL-BORNE THREAT VECTORS.”

intentional misuse by insiders, as well as external attacks on your information infrastructure.

How effective is GajShield's context-based approach to security, in comparison to traditional firewall capabilities?

Based on our context security approach, we have developed a newer Contextual Intelligence Engine that allows to gain advanced visibility and understanding of data transaction over applications that uses network.

Context-based security is a step ahead of traditional firewall capabilities that use deep inspection to identify various data contexts at different levels for advanced security while the Contextual Intelligence Engine understands the application and its context.

With the ability to scrutinise data transactions over the Web, SAAS, Network, etc., combined with Machine Learning, the contextual intelligent engine helps detect anomalies and is proven to reduce false alarm and prevent intentional & unintentional data exploitation with great efficiency.

Ensuring the safety of email communications is a challenge that most companies still find daunting. How is Gajshield helping, in this context? E-mail being the primary means of

business and official communication, it is the most attacked medium to find way into the enterprise's network. Companies of all sizes face this daunting challenge. While E-mail threats move fast, and malicious files look more like normal files that are often used for communication.

GajShield E-mail Security enables enterprise users to communicate securely and protects them from latest email-borne threat vectors like ransomware, advance malware, spam, phishing and data leak using its unique Contextual Intelligence engine with multi-layered approach to security. Our Data Security Firewall identifies attacks and categorises them into various predefined categories to help enterprise analyse threats and take necessary actions based on intelligent and valuable actionable insights.

What are some of the important security aspects that companies need to keep in mind, to secure their data and devices?

Keeping your data secure in today's digital world is critical for your business survival. The first step towards data security is visibility. Be aware of where your sensitive data is residing and get contextual visibility of data in motion. Classifying and categorising data is key to its protection. Ensure that data security policies are setup to protect against breaches of critical data at all points of entries and exists, including your cloud infrastructure. Ensure only authorised users have access to it. Enable contextual visibility to get deep understanding of data and to also connect data to application and user, help you in setting up rules to prevent unauthorised users from sending sensitive data out of your infrastructure.

Setup BYOD policies to minimise network security risks and finally train you employees and make them a key stake holder in your security strategy and not leave it to only technical staff to protect your data. 🙋

RANSOMWARE RECOVERY COST FOR UAE IN 2021 IS \$517,961: SOPHOS SURVEY

THE SURVEY POLLED 5,400 IT DECISION MAKERS IN MID-SIZED ORGANISATIONS IN 30 COUNTRIES ACROSS EUROPE, THE AMERICAS, ASIA-PACIFIC & CENTRAL ASIA, THE MIDDLE EAST, AND AFRICA.

UAE's ransomware recovery cost is \$517,961 in 2021, says Sophos survey

Sophos, a global leader in next-generation cybersecurity, has announced the findings of its global survey, "The State of Ransomware 2021," which reveals that the average total cost of recovery from a ransomware attack has more than doubled in a year, increasing from \$761,106 in 2020 to \$1.85 million in 2021. The average ransom paid is \$170,404. The global findings also show that only 8% of organisations managed to get back all of their data after paying a ransom, with 29% getting back no more than half of their data.

The survey polled 5,400 IT decision makers in mid-sized organisations in 30 countries across Europe, the Americas, Asia-Pacific and Central Asia, the Middle East, and Africa.

While the number of organisations that experienced a ransomware attack fell from 51% of respondents surveyed in

2020 to 37% in 2021, in the UAE, 38% of respondents mentioned a ransomware attack in the last one year, down from 49% in 2020. Globally, fewer organisations suffered data encryption as the result of a significant attack (54% in 2021 compared to 73% in 2020), while in the UAE it dropped to 50%, down from 78% in 2020. The new survey results reveal worrying upward trends, particularly in terms of the impact of a ransomware attack.

"The apparent decline in the number of organisations being hit by ransomware is good news, but it is tempered by the fact that this is likely to reflect, at least in part, changes in attacker behaviors," said Chester Wisniewski, principal research scientist, Sophos. "We've seen attackers move from larger scale, generic, automated attacks to more targeted attacks that include human hands-on-keyboard hacking. While the overall number of attacks is lower as a result, our experience shows that the potential for damage from these more advanced and complex targeted

attacks is much higher. Such attacks are also harder to recover from, and we see this reflected in the survey in the doubling of overall remediation costs."

The main findings of the State of Ransomware 2021 global survey include:

The average cost of remediating a ransomware attack more than doubled in the last 12 months. Globally, remediation costs, including business downtime, lost orders, operational costs, and more, grew from an average of \$761,106 in 2020 to \$1.85 million in 2021. This means that the average cost of recovering from a ransomware attack is now 10 times the size of the ransom payment, on average. In the UAE, the average cost of remediating a ransomware attack is US\$517,961 in 2021, compared to \$696,305 in 2020.

Globally, the number of organisations that paid the ransom increased from 26% in 2020 to 32% in 2021, although fewer than one in 10 (8%) managed to get back all of their data. In the Middle East, 28% of the organisations hit by ransomware paid a



Chester Wisniewski

ransom. "The findings confirm the brutal truth that when it comes to ransomware, it doesn't pay to pay. Despite more organisations opting to pay a ransom, only a tiny minority of those who paid got back all their data," said Wisniewski. "This could be in part because using decryption keys to recover information can be complicated. What's more, there's no guarantee of success. For instance, as we saw recently with DearCry and Black Kingdom ransomware, attacks launched with low quality or hastily compiled code and techniques can make data recovery difficult, if not impossible."

More than half (54%) of respondents believe cyberattacks are now too advanced for their IT team to handle on their own

Extortion without encryption is on the rise. A small, but important 7% said that their data was not encrypted, but they were held to ransom anyway, possibly because the attackers had managed to steal their information. In 2020, this figure was 3%

"Recovering from a ransomware attack can take years and is about so much more than just decrypting and restoring data," said Wisniewski. "Whole systems need to be rebuilt from the ground up and then there is the operational downtime and customer impact to consider, and much more. Further, the definition of what constitutes a 'ransomware' attack is evolving. For a small, but significant minority of respondents, the attacks involved payment demands without data encryption. This could be because they had anti-ransomware technologies in place to block the encryption stage or because the attackers simply chose not to encrypt the data. It is likely that the attackers were demanding payment in return for not leaking stolen information online. A recent example of this approach involved the Clop ransomware gang and a known financially-motivated threat actor hitting around a dozen alleged victims with extortion-only attacks. In short, it is more important than ever to protect against adversaries at the door, before they get a chance to take hold and unfold their increasingly multi-faceted attacks. Fortunately, if organisations are attacked, they don't have to face this challenge alone. Support is available 24/7 in the form of external security operations centers, human-led threat hunting and incident response services."

Sophos recommends the following six best practices to help defend against ransomware and related cyberattacks:

Assume you will be hit. Ransomware remains highly prevalent. No sector, country

or organisation size is immune from the risk. It's better to be prepared, but not hit, rather than the other way round

Make backups and keep a copy offline. Backups are the main method organisations surveyed used to recover their data after an attack. Opt for the industry standard approach of 3:2:1 (three sets of backups, using two different media, one of which is kept offline)

Deploy layered protection. As more ransomware attacks also involve extortion, it is more important than ever to keep adversaries out in the first place. Use layered protection to block attackers at as many points as possible across an estate

Combine human experts and anti-ransomware technology. The key to stopping ransomware is defense in depth that combines dedicated anti-ransomware technology and human-led threat hunting. Technology provides the scale and automation an organisation needs, while human experts are best able to detect the tell-tale tactics, techniques and procedures that indicate an attacker is attempting to get into the environment. If you don't have the skills in house, look at enlisting the support of a specialist cybersecurity company – Security Operation Centers (SOCs) are now realistic options for organisations of all sizes

Don't pay the ransom. Easy to say, but far less easy to do when an organisation has ground to a halt due to a ransomware attack. Independent of any ethical considerations, paying the ransom is an ineffective way to get data back. If you do decide to pay, bear in mind that the adversaries will restore, on average, only two-thirds of your files

Have a malware recovery plan. The best way to stop a cyberattack from turning into a full breach is to prepare in advance. Organisations that fall victim to an attack often realise they could have avoided significant financial loss and disruption, if they had an incident response plan in place. 🚨

AN IN-DEPTH DEFENCE STRATEGY

WERNO GEVERS, REGIONAL MANAGER, MIMICAST MIDDLE EAST, DISCUSSES HOW WHEN IT COMES TO EMAIL SECURITY, IT IS NECESSARY FOR SECURITY PROFESSIONALS TO EVOLVE FROM A PERIMETER-BASED DISCIPLINE TO A MORE PERVASIVE ONE.



Organisations today need a security strategy that's as pervasive and persistent as the threats they work to combat every day. How does

Mimecast help them with this?

In order to develop a comprehensive cybersecurity plan, organisations need to take a risk-based approach. Moving to a risk-based approach helps a team re-prioritise and zero in on what really makes a difference. Organisations also need to implement a defence in-depth strategy, which is essentially a layered approach to cybersecurity. When used in conjunction with the native security features of an organisation's email platform, a defence in depth strategy can support a company's security posture and provide a much greater degree of cyber resilience. Also, with a defence in depth strategy, if one security control proves ineffective, others are in place to fill the breach.

Mimecast's vision is to enable organisations to think bigger and create proactive cyber resilience postures that address the threats at the email perimeter, inside the email network, and also beyond their purview. This will help to eliminate the threats that abuse the trust in their brands. With Mimecast's security solutions, threats are addressed across three zones of control – At the

perimeter, inside the network and organisation and beyond the perimeter – providing businesses with a complete and comprehensive approach.

E-mail is, perhaps, the main entry point used by hackers to orchestrate a cyberattack. In this context, do you think traditional approaches to email security are enough?

The email threat landscape has changed and requires security professionals to evolve from a perimeter-based discipline to a more pervasive discipline, and to think in three distinct zones.

At the email perimeter

Attackers send SPAM and viruses via email and embed URLs to conduct phishing and spear phishing attacks. The email perimeter is a very important place to concentrate controls, whether that's looking for malware or spear phishing, or applying content controls or daily prevention controls in an environment.

Inside the network and the organisation

Attackers can also try to operate inside an email network. They use compromised employee accounts or social engineering to gain the ability to transmit email content from an internal network.

A robust stack of email security technologies can interrogate internal email traffic and inappropriate or malicious content is immediately extracted once detected. Furthermore, employees are susceptible to opening attachments and clicking on links. Awareness training and threat intelligence can help organisations optimise policies and education programs to reduce exposure.

Beyond the perimeter

It's quite easy for attackers to easily impersonate a brand on the internet. They can leverage and ultimately destroy the value and trust of that brand. Even

DMARC GIVES ORGANISATIONS THE POWER TO GOVERN THEIR EMAIL DOMAINS AND HAVE VISIBILITY OVER EMAILS THAT ARE BEING SENT ON THEIR BEHALF."

an unsophisticated attacker can simply register a similar brand domain or host a website or login page and draw customers, partners or the public to it. Protecting organisations from fraudulent activity involves correctly implementing DMARC to protect the domains an organisation owns, combined with proactive hunting for, and takedown of, domain and brand abuse.

Brand impersonation attacks are becoming increasingly common now. What do you think enterprises can do to prevent their "brand" from becoming the victim of an impersonation cyberattack?

Brand exploitation is a major concern for businesses today and many individuals in the region, have been the victim phishing emails, because criminals have successfully impersonated well-known brands such as banks or retailers and duped customers into thinking they were legitimately dealing with the real thing.

Mimecast's fifth annual State of Email Security survey found that 40% of respondents reported an increase in the fraudulent use of their company's brand via spoofed email, while 36% saw an increase in brand impersonation via counterfeit websites.

Domain hijacks and brand impersonation attacks are a very real threat, and it's crucial to have visibility to know what is happening with your brand and be able to protect it. Brand impersonation makes it easy to launch sophisticated attacks using lookalike domains that can easily trick customers, partners and employees.

DMARC is essential for protecting domains owned by the organisation, against email brand exploitation. Tools that protect against online brand exploitation can help identify attack patterns at the preparation stage and block compromised assets before they turn into live attacks. To fully protect a brand, an organisation should consider implementing DMARC along with brand exploitation tools, managed from one integrated system that provides both visibility and proactive remediation.

Tell us more about DMARC and how it can actually help organisations protect their brand.

DMARC gives organisations the power to govern their email domains and have visibility over emails that are being sent on their behalf. This allows security teams to quickly discover and halt any unauthorised emails being sent from their domains, protecting customers, employees, partners and suppliers from potential exploitation by cybercriminals. It also gives companies the ability to instruct those receiving their mails to reject the email if security checks are not aligned.

DMARC is essentially an email authentication standard that helps businesses fight the rising threat of brand exploitation, including email phishing attempts and business email compromise attacks. It builds on existing SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail) protocols by adding a critical reporting element and a blocking mechanism. DMARC analyses SPF and DKIM results to instruct an inbound mail server what to do with messages that fail these checks. 📧

THALES ANNOUNCES NEW SOLUTIONS TO HELP ORGANISATIONS DISCOVER, PROTECT AND CONTROL SENSITIVE DATA IN MULTICLOUD ENVIRONMENTS

THALES HAS ANNOUNCED NEW DATA PROTECTION SOLUTIONS FOR GOOGLE CLOUD, MICROSOFT AZURE, AND AMAZON WEB SERVICES, SOLIDIFYING ITS ROLE AS A TRUSTED THIRD PARTY FOR MULTICLOUD DATA SECURITY.

With each cloud provider having unique data protection mechanisms and key management offerings, multicloud data protection presents a complex security challenge for organisations. Thales' latest cloud data security solutions allow customers to maintain control of and manage their encryption keys, as well as manage access and authentication across hybrid and multicloud environments.

"These capabilities are critical to cloud migration and security, especially with such accelerated growth in this area," said Sunil Potti, Vice President and General Manager of Google Cloud Security. "True to our mission, we have forged this collaboration with Thales to further protect our customer's most sensitive information. We are

empowering customers to leverage the full potential of Google Cloud technology for sensitive workloads, by utilising the Customer-Managed Encryption Key-integrated GCP services, CipherTrust Cloud Key Manager and SafeNet Trusted Access for access management and authentication from Thales. This will enable enterprises to deal with a fluid and dynamic business environment where protecting sensitive data in the cloud is of extreme importance."

SIMPLIFYING MULTICLOUD SECURITY

As customers look to reap the rewards from multicloud environments, Thales is making it easier to ensure protection against reputational risk and financial penalties arising from a cloud data breach. As such, customers will benefit from enhanced capabilities to Discover, Protect and

Control sensitive data across multicloud environments, including the ability to:

Discover Sensitive Data in the Cloud and On-Premises

Thales Data Discovery and Classification automates the discovery, classification and protection of data in the cloud and on-premises using automation policies that identify sensitive data and protect the data with encryption or tokenisation. These capabilities have now been extended to the discovery and classification of data in Amazon Web Services S3 buckets and Azure Blob storage.

Protect Sensitive Data and Workloads in the Cloud

To address both the complexity of where data is stored and to help ensure data sovereignty in a multicloud environment,



effective encryption and tokenisation is needed. Specific new data protection capabilities for cloud platforms include:

- CipherTrust Transparent Encryption for advanced encryption and access controls, protects data in Amazon Web Services Simple Storage Service (S3)
- Encryption of Kubernetes secrets and Google Anthos Service Mesh signing keys

Control Access to Applications and Sensitive Data in the Cloud

The accelerated adoption of encryption has led to the need to manage a far larger number of encryption keys across both traditional data stores and multicloud environments. Thales has enabled new capabilities that allow organisations to control access to data and ownership of their encryption keys, including:

- Thales is also offering CipherTrust

Cloud Key Manager support for Google Cloud's External Key Manager (EKM), building on the existing CipherTrust Key Broker for Google Cloud EKM which is part of the Thales Data Protection on Demand cloud-based platform.

Secure and Protect access at the Login Point

Compromised identities pose one of the greatest risks for data breaches:

- SafeNet Trusted Access integrates out of the box with Google Workspace, Azure and AWS, enforcing the appropriate access controls and authentication for privileged and regular users.
- SafeNet Trusted Access is offering new abilities to provide authentication and authorisation for APIs and for applications not using industry-standard protocols such as SAML and OIDC.

"The proliferation of multicloud computing has created new organizational challenges in managing data across many different cloud environments. Whilst organisations have benefited from scalability and speed to market thanks to the power of cloud, the ever expanding IT cloud landscape has added greater complexity to data management and security", said Sébastien Cano, Senior Vice President, Cloud Protection and Licensing activities at Thales.

"In a post pandemic, highly regulated world, it is even more important for organisations to understand what data they have, where it sits, who can access it and the risks associated with managing it. Only once an organisation understands all of these data lifecycle aspects, can they ensure that it is secured and managed correctly," he added. 🧑🏻‍💻

MULTI-CLOUD REQUIRES IMPECCABLE DIGITAL HYGIENE

BY: DAVE RUSSELL, VICE-PRESIDENT,
ENTERPRISE STRATEGY AT VEEAM SOFTWARE

Gartner estimates that by 2022, 75% of enterprise customers using cloud infrastructure as a service will adopt a deliberate multi-cloud strategy. Up from 49% in 2017, this is a fast-growing trend, which shows little sign of abating as businesses continue to 'mix and match' the services provided by the big four hyperscalers – AWS, Microsoft Azure, Google Cloud Platform, and Alibaba. The truth is that there is, and in the IT world this is a tale as old as time. Infrastructure evolves and expands organically, based on the need for short term fixes and challenges posed by managing increasing data volumes. The pandemic underlined this fact in a big way. According to Veeam's Data Protection Report 2021, 50% of CXOs in Saudi and 52% in UAE said that the need to maintain operations during the pandemic had held back their strategic digital transformation initiatives. It is only now that we will see a shift as businesses move beyond the crisis stage of their Covid-19 response and start to look at how the digital infrastructure and skills they acquired through short-term necessity can be evolved into a coherent, longer-term vision.

The question I would post is, how many have a deliberate multi-cloud strategy? Yes, many enterprises will have weighed up the pros and cons of working with each cloud provider and implemented a Cloud Data Management strategy to ensure they can

manage and protect data across multiple public cloud platforms. But we must not pretend that a significant number are likely to have found themselves working with multiple cloud providers, based on factors such as what platforms their partners use, through mergers and acquisitions, or in an attempt to contain spiralling costs. This is where the risk of multi-cloud can begin to offset the benefits.

Send in the digital health inspectors

Multi-cloud brings a number of challenges in terms of cloud security, skills, and cost optimisation which businesses must be aware of before investing heavily in this as a strategy. Focusing on security first, so often cybersecurity vulnerabilities can be traced back to low levels of digital hygiene – a problem that is exasperated by using multiple cloud providers. In an ideal world, businesses would all have the required digital hygiene to successfully manage a multi-cloud environment, reaping the benefits of scalability and diverse capabilities this can bring. But in the real world rather than the ideal world, many businesses are still challenged by shadow IT and employees who require more extensive training when it comes to handling data compliantly, being more savvy when it comes to spotting phishing links, and using strong, varied passwords that they change regularly.

The public cloud opens up an array of

exciting opportunities for organisations looking to consume Software as a Service (SaaS) and manage the exploding data volumes which have challenged IT departments globally. However, there is a feeling among IT teams that the public cloud has not completely fulfilled the promise of being cost-effective. In fact, for many cloud costs are spiralling out of control. So, it stands to reason, that if it's difficult to contain the costs of using one public cloud, it certainly isn't any easier to contain the costs of using multiple clouds. This is where having a cohesive Cloud Data Management strategy comes into play. Businesses need to be honest with themselves and ask whether they have adopted an intentional multi-cloud strategy, or did it just happen? If it's the latter, that is fine, but it's time to conduct a full review of your cloud provision, and ensure you have the required skills on board to maximise your use of each cloud, contain your storage costs, and to ensure data is fully protected across all infrastructure.

Businesses looking to deliberately form a multi-cloud strategy must first ensure that their standards of digital hygiene – including cybersecurity protocols, tracking, clear roles and responsibilities – are fit for purpose. This is fundamental to the success of reaping the very real benefits of, while managing the potential risks in terms of cloud security and cost containment. 🧑

Cyberattacks don't stop at your email perimeter. Your security can't either.

Phishing campaigns and business email compromise (BEC) grew by 54% and 67% respectively this past year proving that email continues to be the #1 attacked vector by cybercriminals.

Prevent Malicious Emails with DMARC

- Gain full visibility and governance across all email channels
- Authenticate email messages and improve deliverability
- Block inbound attacks and protect brands against abuse
- Publish a policy that instruct ISP's to deliver or delete emails



**DMARC
Resources
& Free Trial**

info.mimecast.com/dmarc-resources



mimecast



Security-Driven Networking, everywhere you need it.

Protect the possibilities
with Secure SD-WAN.

