WWW.TAHAWULTECH.COM **ISSUE 65 | JUNE 2022**





Manage your network centrally from any location, without the need to set up a server. Because Nuclias Cloud devices only need plugging in and powering up, it's perfect for businesses that don't have trained IT professionals.

Who needs Nuclias Cloud



SMBs & Large Enterprises



Retail Chains



Hospitality



Education

CONTENTS

Security









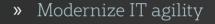
- 6 News roundup from the world of cybersecurity
- 32 Dell Technologies-Intertec Systems event roundup
- Danny Allan, CTO & Claude Schuck, Regional Director, Middle East, at Veeam, on the ransomware trends report which reveals that businesses are losing the battle when it comes to defending against ransomware attacks.
- Israel Barak, Chief
 Information Security
 Officer, Cybereason
 on XDR and why it's
 taking the security
 world by storm



Today's IT agility is built on observability.

SolarWinds® Hybrid Cloud Observability helps ensure services and online applications are available, operate cost effectively, and deliver a fantastic and predictable digital experience.

000



» Accelerate cost savings and time to value

» Resolve issues faster with deep visibility and context

» Improve user experience and service availability

» Value across IT Ops, Dev Ops, and security



Learn more about Hybrid Cloud Observability and how we're re-envisioning the solutions you need to drive business results.

Visit solarwinds.com to learn more.



EDITOR'S NOTE



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

> Anita Joseph Editor

EVENTS





THE DATA DILEMMA

Data Sovereignty is well-acknowledged and extremely vital aspect of cybersecurity. In fact, data sovereignty has become a matter of concern for many policymakers who feel there is too much control ceded to too few places, too little choice in the tech market, and too much power in the hands of a small number of large tech companies. This quest for sovereignty is even more important considering that the pandemic highlighted the EU Member States' dependencies on vaccines, protective masks, and increasingly on digital technology developed by GAFAM

(Google, Amazon, Facebook, and Microsoft).

In our cover story this

month, Sebastien Pavie, VP,
Data Protection Solutions,
Southern Europe & Middle
East at Thales, tells us all
how the problem of data sovereignty is
closely related with the cloud. Data sto

closely related with the cloud. Data stored in cloud computing services may be under the jurisdiction of more than one country's laws. Different legal requirements regarding data security, privacy, and breach notification could occur, depending on where the data is being hosted or who is controlling it.

In our focus interview section, Piers

Morgan, VP & GM International at eSentire, discusses the company's approach to MDR and their partnership with MMA Infosec. He says that in terms of the region, "we're seeing exponential growth for our own business, but the only reason that is growing is because the companies within this region are also growing and becoming more globally visible and stretching their own wings."

In another interview, Israel Barak, Chief Information Security Officer, Cybereason, discusses XDR and how it's taking the cybersecurity world by storm. "XDR is about

> not only bringing in all that data from all those different places in the enterprise and making sure that we have visibility into everything that is happening across the enterprise, endpoint, cloud,

identity and access in one place, but also being able to drive automation-automation in analysing the data, detecting the threat in as close to real time as possible."

That's not all: we have the usual opinion, insight and news roundup columns, to make sure you don't miss out on the latest developments and trends in the cybersecurity industry. Happy Reading!

FOUNDER, CPI Dominic De Sousa (1959-2015)

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

Publishing Director Natasha Pendleton

natasha.pendleton@cpimediagroup.com

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.comm

OnlineEditor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

PRODUCTION AND DESIGN
Senior Designer
Analou Balbero

analou.balbero@cpimediagroup.com

webmaster@cpimediagroup.com

DIGITAL SERVICES

Web Developer

Adarsh Snehaian

DATA SOVREIGNTY HAS

BECOME A MATTER

OF CONCERN FOR

POLICYMAKERS.

Published by



Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAF

Tel: +971 4 5682993

© Copyright 2022 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.

SOPHOS NAMED LEADER IN 2022 KUPPINGERCOLE LEADERSHIP COMPASS FOR ENDPOINT PROTECTION, DETECTION & RESPONSE

Sophos, a global leader in next-generation

cybersecurity, has announced it has been named a leader in the 2022 KuppingerCole Leadership Compass for Endpoint Protection, Detection and Response. It is commended as an Overall Leader, sweeping all product, innovation and market leadership ratings. "An increasing number of organisations are being hit with ransomware, and the average ransom payment rose nearly fivefold to more than \$800,000 last year, according to the State of Ransomware 2022," said Raja Patel, senior Vice-President of products at Sophos.

"There's a lot at stake, and no organisation is off limits. This KuppingerCole recognition is validation that Sophos is delivering industry-best protection against ransomware and other advanced cyberthreats."

Sophos Intercept X provides multiple layers of security, combining antiransomware technology, deep learning Artificial Intelligence, exploit prevention, and active adversary mitigations. Intercept X with XDR extends protection to include detection, investigation and response capabilities beyond endpoints and servers, integrating additional context to create



the industry's richest data set. Customers can easily manage these capabilities in the cloud-native Sophos Central platform, or can choose to have them managed by Sophos MTR, a threat hunting, detection, investigation, and response service that provides a dedicated 24/7 security team to rapidly identify and neutralise sophisticated and complex threats.

EMT DISTRIBUTION PARTNERS WITH THREAT DETECTION SOFTWARE VENDOR GATEWATCHER FOR MEA

emt Distribution, a major IT & IT

Security product distributor based on security, IT Management, and analytic solutions, has announced an enhanced partnership with Gatewatcher, Europe's leading cybersecurity software company specialising in the detection of advanced cyber threats.

Gatewatcher publishes a suite of solutions based on next-generation technologies that effectively protect organisations against intrusions. Thanks to a 360° view of cyber threats, Gatewatcher's solutions, based on artificial intelligence, offer a flexible (cloud, on premise, hybrid), and scalable approach. They also facilitate the operations of cybersecurity teams for a better efficiency in the prioritisation of their remediation actions.

"As cyberattacks are becoming more complex to detect day-by-day, cybersecurity experts have increasing challenges protecting their organisations especially their main and critical gateway which is their network. AionIQ®, Gatewatcher's detection and response platform (NDR), identifies malicious

GATEWATCHER

PARTNERSHIP ANNOUNCEMENT

actions and suspicious behaviours based on a mapping of all assets present on the IS. The combination of this capability with unprecedented performance in analysing malicious behaviour, even in the case of encrypted network flows, provides a 360° modelling of the level of cyber risk associated with each connection between assets and users. AionIQ® delivers an unparalleled level of detection and visibility of cyber threats, whether known

or unknown: Ransomware, APTs, zero-day vulnerability exploits, etc. Gatewatcher's dedication on research and development of an uncommon solution will help many organisations and large enterprises in the region to maximise their cybersecurity. We are so thrilled to announce this partnership and looking forward to helping many organisations with help of our fantastic channel partners in the region!" said M. Mobasseri – CEO, emt Distribution.

CHECK POINT SOFTWARE TECHNOLOGIES ACHIEVES NEW COMMON CRITERIA CERTIFICATION

Check Point Software Technologies

Ltd. a leading provider of cyber security solutions globally, has announced the successful completion of a new Common Criteria (CC) certification. This achievement marks the important recognition of Check Point's ability to meet or exceed the security requirements of the 31 Nations who are members of the Common Criteria Recognition Agreement (CCRA). Purchase decisions by government and closely related industry, including critical infrastructure often require certification through Common Criteria.

Common Criteria certification is recognised by governments around the world as the standard for validating the security claims of products before purchase. It provides the criteria for independent, scalable, and globally recognised security inspections for IT

products. The new CC protection profile certification complements Check Point CC EAL4+ certification, reaffirming Check Point's commitment to maintain the highest security standard required by governments worldwide.

COMMON CRITERIA **CERTIFICATION IS RECOGNISED BY GOVERNMENTS** AROUND THE WORLD AS THE STANDARD SECURITY CLAIMS OF **PRODUCTS BEFORE** PURCHASE.



EYAL MANOR

"These certifications underscore Check Point's ability to protect global entities and comply with the latest approved standards for protecting and securing IT infrastructure and information while providing the secure services required to run a business." said Eyal Manor, Vice President of Product Management at Check Point. "Check Point is focused on delivering innovative solutions that consistently meet and exceed the requirements to provide the highest level of security globally," he added.

EVANSSION AND CYBER RANGES ANNOUNCE DISTRIBUTION PARTNERSHIP TO BOOST CYBER RESILIENCY IN THE MIDDLE EAST

Evanssion, a value-added distributor

(VAD) specialised in Cloud Native and Cybersecurity across the Middle East and Africa, has announced its distribution partnership with CYBER RANGES by Silensec, a next-generation militarygrade full-content-lifecycle cyber range for the development of cyber capabilities and the assessment of competencies and organisational cyber resilience. As per the terms of the partnership, Evanssion will deliver the full extent of CYBER RANGES' portfolio of world-class cybersecurity training and capability development exercises to enterprises in the Middle East region.

Evanssion together with its extensive partner network will create awareness and large-scale cyber drills for

organisations in the region to test their cyber resiliency through CYBER RANGES offerings. The distributor will also hold training sessions for its partners to help them become well- versed with CYBER RANGES solutions to be better equipped to position it to regional customers.

Commenting on the collaboration, Navneeth Ramanan, Assistant Vice-

EVANSSION WILL DELIVER THE FULL **EXTENT OF CYBER** RANGES' PORTFOLIO **OF CYBERSECURITY** TRAINING & CAPABILIT **DEVELOPMENT EXERCISES.**



RAMANAN

President - Sales for Evanssion, said, "We are thrilled to sign up with CYBER RANGES for the Middle East region. Adding the domain of cyber range solutions to Evanssion's portfolio enables us to present CYBER RANGES and its world-class offerings to the region at a time when cybersecurity is a top priority for every business across verticals."

"We will work closely with our partners to promote CYBER RANGES exercises and play a key role in empowering regional businesses to boost their cybersecurity posture, capability and resilience," he added.

KASPERSKY CYBER IMMUNITY BECOMES TRADEMARK IN THE US

kaspersky

The Cyber Immunity concept developed by Kaspersky alongside its KasperskyOS operating system, is now a trademark. Having this trademark further reinforces Kaspersky's unique approach within the IoT and connected devices market.

Cyber Immunity embodies the secureby-design approach which helps tackle cybersecurity vulnerabilities in the very early stages of software development. Kaspersky's Cyber Immunity concept implies that the overwhelming majority of cyberattack types are ineffective and cannot affect a system's critical functions in the usage scenarios specified at the CYBER IMMUNITY
EMBODIES THE
SECURE-BY-DESIGN
APPROACH WHICH
HELPS TACKLE
CYBERSECURITY
VULNERABILITIES
IN THE VERY EARLY
STAGES OF SOFTWARE
DEVELOPMENT.

design stage. Cyber Immunity can be achieved by using KasperskyOS and following certain methodology while creating a solution, such as defining security goals and assumptions and ensuring they are accomplished in all usage scenarios, the isolation of security domains and the control of interaction among them, and the reliability of the solution's whole trusted computing base.

"Registering the Kaspersky Cyber Immunity trademark on an international scale is the result of our consistent efforts to create a new market for systems with built-in cyberthreat resistance. This recognition is important for our team but also for market analysts and customers. From now on, the first IoT gateway, Kaspersky IoT Secure Gateway 100, and all our upcoming KasperskyOS-based products have a unique feature, recognised all over the world. Kaspersky Cyber Immunity is an essential instrument for digital transformation," said Andrey Suvorov, Head of KasperskyOS Business Unit.

AXIS LAUNCHES EXPERIENCE CENTER



Axis Communications announced the

opening of an Axis Experience Center (AEC) in Dubai. As the first experience center in the Middle East & Africa (MEA) region, the center has been designed to offer visitors an intimate look at the wide range of network and security solutions offered by the

world's leading surveillance services provider. They will also get a unique opportunity to visualise the application of these solutions in use cases ranging from smart city traffic monitoring and vehicle access control to body-worn and deployable surveillance solutions.

"Bringing the Axis experience to Dubai



is a testament to the region's reputation as a hub for raw innovation and ideas. With landmark events such as Expo 2020, conversation and collaboration are put front and center. An Axis Experience Center gives us the space and opportunity to engage with clients and partners, and work together to design and develop the solutions that we will use to realise the smart, sustainable cities and systems of the future," said Ettiene van der Watt, Regional Director – Middle East & Africa at Axis Communications.





Deterministic Protection Platform



Protect full attack surface



Only allows correct execution



Automated runtime protection



Ready-only probe



Zero attacker dwell time



Works with any server

"The world has been far too patient with security vendors who claim to protect against the unyielding ransomware and remote code execution attacks crippling our businesses. Traditional approaches simply do not work. Any CISO or CIO needs to be able to walk into the CEO's office or the boardroom and confidently say that they can not only protect against these attacks but can stop them, within milliseconds, before they do any damage. Virsec is the only company that can give these tech leaders the confidence to say 'Yes!"

— John Chambers,
Former Chairman & CEO, Cisco, and CEO, JC2 Ventures

Recognized Security Leaders

Gartner





ARN Innovation Awards 2021

MITRE





tahawultech.com CISO50 & Future Security Awards 2021

HOW TO PROTECT YOUR ORGANISATION FROM BECOMING ANOTHER RANSOMWARE STATISTIC

SANDRA HATTAB. CYBERSECURITY CONSULTANT, AXON TECHNOLOGIES

ong gone are the days when a set of logical cybersecurity safeguards would be considered sufficient to protect an organisation from threats of ransomware. With the growing scale and sophistication of this emerging class of cyberattacks, if you think your organisation has all what it takes to protect itself against a ransomware attack, I urge you to reconsider. Ransomware criminals have been employing multi-pronged attacks that involve not just encrypting files and locking operating systems, but also exfiltrating and destroying data and executing denial of service (DoS) attacks on the underlying infrastructure. No organisation of any size is immune to this class of cyberattacks.

The Lockheed Martin Cyber Kill Chain offers cyber defenders a model they can leverage to understand an organisation's IT environment, the weaknesses that may allow an attacker to compromise its systems, and the mitigations that should be put in place. This framework inspects a ransomware attack lifecycle and breaks it down into seven key steps. Understanding each step in the kill chain helps inform what protection mechanisms should be applied.

SETTING UP
EFFECTIVE SECURITY
MONITORING
& ANALYSIS
FOR INCOMING
WEB TRAFFIC
ENSURES THAT
ONLY LEGITIMATE
VISITORS ARE
ALLOWED.

Beyond just the technology, a deep dive into process and people-oriented cybersecurity protection is key to thwarting ransomware attacks and preventing their advancement to the next steps in the chain. In what follows, we break down these protections based on the Kill Chain framework.

Almost all ransomware attacks begin with Reconnaissance. Attackers investigate

their target using available sources of information with activities like network scans, browsing websites for directory information, looking for email addresses of executives, etc... with the goal of learning as much as possible about the intended target to find potential avenues of attack. Once a target is identified, recon about what avenues of compromise can be exploited are also inspected. This could take the form of vulnerabilities or misconfigurations in the target system. To prevent your environment from giving away information about applications, data, or weaknesses in the underlying IT infrastructure, it is recommended that organisations take proactive steps to assess the security architecture of their infrastructure and its design and that the implemented logical controls meet industry security recommendations. Setting up effective security monitoring and analysis for incoming web traffic ensures that only legitimate visitors are allowed on a web application and prevents malicious web crawling tools from achieving recon goals. Although security monitoring and analysis is mainly a detective process, a SOAR capability provides protection mechanisms



through threat data collection and automated response to security events.

Weaponization occurs once a vulnerable pathway is found into the target organization and an exploit is crafted to suit the vulnerability detected. Secure coding principles should be an integral aspect of software development lifecycle. In addition, security reviews and tests (ex. code reviews, vulnerability scans, and penetration testing) should be carried out periodically on existing applications to identify weaknesses, and a shift left approach to security requirements should be implemented as part of any new system acquisition and software development project management activities. A robust vulnerability and patch management program will ensure that weapons targeting identified vulnerabilities will fail to achieve their objective. A cybersecurity maturity assessment can identify gaps in the implementation of these protection mechanisms and provide recommendations to achieve target state

protection requirements.

Delivery involves transmitting the weapon to the target system. This can occur in any number of ways, including avenues as simple as sending a phishing email to a user, or a more complicated transmission medium like an exploited service running on a system that allows for the remote execution of malware. The best line of protection against this is strong user awareness. Organisations that ensure users are periodically trained on cybersecurity aspects, run campaigns to raise awareness, and execute phishing simulations are best equipped to evade threats of ransomware. Security reviews and testing can reveal security misconfigurations that can be then corrected by a security engineering team.

Exploitation is the execution of the weapon delivered. It takes some form of control over the exploited system. The traditional goal of most attackers is to be able to obtain escalated access to an exploited system and have complete

control, though lesser forms of access can still be useful for activities like data exfiltration. Access control is paramount at this step. A thorough assessment of existing access control procedures will yield a set of recommendations that help achieve strong protection against this step of the kill chain.

Installation involves the attacker finding a way to maintain persistent access to the compromised system, which means that if a system admin identifies and removes the malware installed, the goal is to still have a covert way to access the compromised system, Command and Control, or C2. is the step in the kill chain where the compromised system establishes a connection to a command-and-control environment. This remote connection is how the attacker interacts with the compromised system or the location where the data stolen is sent to. Ensuring that security logs are protected, monitored, and analysed for suspicious activities. connections, and abnormal behaviour will play a big role in detecting and preventing the success of the actions taken in these two stages of the attack.

Actions on Objectives is the final step in the chain where the intended goal of the whole attack is achieved and where all the previous steps culminate. This is where data exfiltration or data destruction usually occur. Here, a successful data classification and data loss prevention program will protect the organisation's crown jewels from falling in the wrong hands. This would typically include the establishment of a data classification scheme, classification of structured and unstructured data, enforcing the use of asset labelling, and implementation of a data loss prevention program. Additionally, data minimisation principles that require the collection and retention of only the data necessary for accomplishing business missions would greatly prevent the leakage of information that might otherwise be unnecessarily stored without an explicit business need or defined lifetime.

ADDRESSING DATA SOVEREIGNTY

SEBASTIEN PAVIE, VP, DATA PROTECTION SOLUTIONS, SOUTHERN EMEA AT THALES, TELLS ANITA JOSEPH IN AN EXCLUSIVE INTERVIEW WHY DATA SOVEREIGNTY HAS BECOME CRITICAL FOR POLICY-MAKERS WHO INCREASINGLY FEEL THERE IS TOO MUCH CONTROL CEDED TO TOO FEW PLACES, TOO LITTLE CHOICE IN THE TECH MARKET AND TOO MUCH POWER IN THE HANDS OF A SMALL NUMBER OF LARGE TECH COMPANIES.

n the last few years, the volume and value of digital data has increased tremendously. As modern organisations and nation states are pursuing their digital transformation strategies, they become reliant upon digital platforms as part of their operations. While digitalisation has brought considerable opportunities, new risks have also emerged. Data theft and compromise is real risk for all organisations, costing millions of dollars every year.

The World Economic Forum estimates that over 92% of all data is stored on servers owned by US-based companies. The sense of losing control

over your data is an escalating anxiety for all businesses and governments all over the world. The fear of foreign entities compromising sensitive data has brought into discussion the concept of data sovereignty and how businesses can ensure that their valuable data doesn't fall into the wrong hands without permission.

What is data sovereignty?

The World Economic Forum defines data sovereignty as "the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create." Data sovereignty emerged as a need



for "strategic autonomy" of the European institutions, seeking to reduce "dependencies." A recent paper authored by the heads of Germany, Estonia, Finland, and Denmark notes that EU needs to "foster the Digital Single Market in all its dimensions where innovation can thrive and data flow freely. We need to effectively safeguard competition and market access in a data-driven world."

The guest for digital sovereignty is therefore a goal shared by companies, public authority stakeholders and, more recently, Internet users, citizens, and consumers. Data sovereignty has become a concern for many policymakers who feel there is too much control ceded to too few places, too little choice in the tech market, and too much power in the hands of a small number of large tech companies. This guest for sovereignty is even more important considering that the pandemic highlighted the EU Member States' dependencies on vaccines, protective masks, and increasingly on digital technology developed by GAFAM (Google, Amazon, Facebook, and Microsoft).

In the wake of the movement initiated by Europe and followed by the United States, governments are implementing privacy policies to meet new requirements in terms of confidentiality, support and security of data processing. Data processing poses a challenge in terms of sovereignty, requiring the introduction of an appropriate legal framework, as reflected by changes in European laws and in the Middle East.

The problem of data sovereignty is closely related with the cloud. Data stored in cloud computing services may be under the jurisdiction of more DIFFERENT LEGAL
REQUIREMENTS
REGARDING
DATA SECURITY,
PRIVACY,
AND BREACH
NOTIFICATION
COULD OCCUR,
DEPENDING ON
WHERE THE DATA
IS BEING HOSTED
OR WHO IS
CONTROLLING IT.

than one country's laws. Different legal requirements regarding data security, privacy, and breach notification could occur, depending on where the data is being hosted or who is controlling it.

As you consider where to store data—on-premises or in one or more public cloud providers—you need to consider where the data will be stored, what laws are applicable to these geographic locations, and whether storing data in a certain location will be beneficial or harmful to your business.

Companies using cloud infrastructure must address data sovereignty analysis holistically. Data sovereignty is not an issue that can be addressed only by the Chief Information Officer. IT security, legal department, procurement, risk managers, and auditors must all be

involved in risk management and governance processes.

At this point it is essential to understand that data sovereignty is different than data localisation.

- Data sovereignty is a governmental policy or law noting data is subject to the data and privacy laws of a specific geographical location.
- Data localisation is a governmental policy or law that specifies where governments can locate data. An example is the EU GDPR. It states that European countries should host all personal information collected on European citizens within the EU within the EER, EU, or several other specified countries.

How are businesses affected by data sovereignty laws?

The invalidation of the EU-US Privacy Shield in 2020 by the Court of Justice of the European Union through the Schrems II ruling was the event that triggered the discussion about data sovereignty. Although the EU and the US have already agreed to a new Trans-Atlantic Data Privacy Framework to sufficiently manage such data exchanges, it should be noted that the Schrems II ruling affects all data transfers between EU and third countries, including the states in the Middle East.

The EU-US Privacy Shield worked as an overall legal protection umbrella under which global enterprises were safe to work and transfer data between the European Union and the United States. It is estimated that over 5,000 organisations, their subsidiaries, and their suppliers were affected by the ruling threatening a portion of the \$1.3 trillion in yearly transatlantic trade.

The EU-US legal digital sovereignty

challenge is the most visible example, but it is by no means the only point of contention. Around the world, even between EU member states, digital sovereignty is becoming an issue.

The surge in privacy regulation in recent years has prompted a shift towards localisation and the containment of data within state boundaries. As a response, technology giants are building localized data centers to circumvent geographical barriers to business, while providing complete oversight over data storage and access to meet the compliance requirements. With more and more countries worldwide enacting similar data protection and privacy laws and regulations, the issue of data sovereignty and digital destiny remains a multifaceted one.

The Middle East in the wake of sovereignty concerns

Following the trend across many countries for greater data protection, new data protection laws are enacted by various states in the Middle East.

On the other hand, in a hyper connected digital market, all businesses in the Middle East can potentially hold data or transfer data of European citizens, which implies taking into account some requirements for data transfers enacted in the EU. Having a knowledge of the governing framework and the supporting Standard Contractual Clauses (SCCs) is crucial to ensure an uninterrupted data flow between Middle East companies and EU nations.

The key challenges of data sovereignty

Data sovereignty has raised questions for CIOs considering their cloud



DATA
SOVEREIGNTY
HAS RAISED
QUESTIONS FOR
CIOS CONSIDERING
THEIR CLOUD
STRATEGY,
GOVERNANCE,
AND RISK
MANAGEMENT.

strategy, governance, and risk management. When you expand your data to additional regions, whether for production data, data backups or disaster recovery, you must be mindful of data sovereignty.

Data at rest

Before you even think about compliance, regulations, and rules, one of the initial things to consider is how and where you store your data. The first choice is whether to store data on premises or in the cloud. In the cloud, data sovereignty becomes more complex.

If you migrate your data to the

cloud, as most companies do, you will need to select options for replication and backup, which in many cases will involve storing data in another geographical location. The cloud provider may or may not allow you to select the region where backups or replicas will be stored. You should ensure that you are able to specify the region in which data will be stored and understand the regulatory requirements of each region.

The challenge is not only where the sensitive data resides geographically, but even who has access to sensitive data inside a corporation. For example, according to the recent Schrems II decision, if an employee based in the United States accesses sensitive EU protected data inside his own organisation, this could be considered an "export" of sensitive data and an infraction of the GDPR rules.

Data in transit

Organisations often overlook data in

FOR AN
ORGANISATION
TO DECIDE
WHICH LEVELS
OF PROTECTION
AND CONTROLS TO
USE, IT MUST BE
ABLE TO DISCOVER
DATA WHEREVER
IT RESIDES AND
CLASSIFY IT.

transit. However, it is essential if you consider the following questions:

- How often do you transfer data between geographical regions?
- From where and to where is data transferred?
- What type of data is typically transferred?

You should understand your data flows because they relate to how data is being collected and processed. It is especially important to understand data sovereignty in the source and destination region, and if there are legal issues, adjust your data flows to ensure data ends up in the most appropriate legal jurisdiction.

However, in a multi-cloud organisation, taking care of data sovereignty is easier said than done. This is especially difficult when a majority of enterprises rely heavily on third party service providers for intelligent insight and competitive advantages extracted from often regulated company data.

The three pillars of digital sovereignty

Thales considers data sovereignty as one of the three pillars towards an effective digital sovereignty in support of a successful cloud strategy. The other two pillars are operational sovereignty and software sovereignty.

Data sovereignty means maintaining control over encryption and access to your sensitive data to ensure it doesn't fall into the hands of a foreign entity without express permission resulting in non-compliance with regulations.

Operational sovereignty means giving an organisation the visibility and control required to ensure that criminals cannot access, or prevent you from accessing, your valuable data, such as in the case of privileged user access or a ransomware attack.

Software sovereignty means running workloads without dependence on a provider's software, offering the freedom to store and run workloads wherever desired to maximise performance, flexibility, and overall resilience.

DISCOVER, PROTECT, AND CONTROL YOUR SOVEREIGNTY

Organisations can achieve data software and operational sovereignty with automated risk assessment and the centralised protection and control of sensitive data across cloud and on-premises

Discover

systems.

For an organisation
to decide which levels
of protection and controls
to use, it must be able
to discover data wherever
it resides and classify it. This
means scanning all on premises
and cloud repositories for structured
and unstructured data, which can be





IT IS ESPECIALLY IMPORTANT TO UNDERSTAND DATA SOVEREIGNTY IN THE SOURCE AND DESTINATION REGION.

in many forms, including files, databases, and big data. Data sovereignty starts with finding your sensitive data before criminals do.

Protect

Once an organisation knows where its sensitive data is, it should protect that data with measures such as encryption. For encryption to successfully secure sensitive data, the cryptographic keys themselves must be secured, managed, and controlled by the organisation.

Control

Finally, the organisation needs to control access to its data and centralise key management. Every data sovereignty or privacy regulation and mandate requires organisations to be able to monitor, detect, control, and report on authorised and unauthorised access to data and encryption keys.



ell us about ISS Security and its presence in the region
ISS was, and remains, a pioneer in the world of intelligent video solutions.
Our ISS SecurOS platform is recognised globally as one of the most robust and flexible video management platforms available. ISS was, also, literally, among the very first firms to write algorithms for video analytics - a lead it has kept up and where it continues to innovate with advanced neural network and Al methodologies.

The company was founded 25 years ago, and has been operating in the Middle East for the past decade. In addition to our offices in Dubai and Abu Dhabi, we have sales and technical offices in Riyadh and Doha.

Honestly, we love being a player on the Middle East pitch, where we find some of the most sophisticated and demanding customers in the world.

What does your portfolio of products and solutions look like?

Our portfolio of products and solutions are all customer-use focused and forged in the fires of implementations and references from all around the world. One the beauties of ISS is to take experiences from major enterprise installations and translate them - very much into local language (literally), customs and demands. From security to operational efficiency to compliance, we'll work with the camera as the key (not by any means the only) sensor to meet integrator and end user needs.

What are some of the latest trends in the security surveillance market today? How are customer preferences changing?

We love the way the market is shifting. While hardware has become



increasingly viewed as a commodity, the focus on surveillance has now become fixed on analytics; and the ability of analytics to lead to action and the collection of data points that lead to intelligence. ISS simply excels in these arenas. Further, the magic word in surveillance begins with the letter "i". That word is "integration". With best of breed technologies being called for from end users [not "just"]

THE FOCUS ON
SURVEILLANCE HAS
NOW BECOME FIXED
ON ANALYTICS AND
THE ABILITY OF
ANALYTICS TO LEAD
TO ACTION AND THE
COLLECTION OF DATA
POINTS THAT LEAD TO
INTELLIGENCE.

good enough" technologies), reducing risk in implementation is paramount. In that area, ISS is the integrators' friend - bar none - both in our technology infrastructure and in our famous and relentless customer service.

Tell us about your latest award. What is it in recognition of?

The ISS Under Vehicle Surveillance System - ISS-UVSS - is simply second-generation revolutionary. It's innovative (four US patents owned by ISS are employed), sleek but incredibly rugged, simple to install and the most effective scanning available. And it's a third to a half cheaper than the aging first generation incumbent.

What are your plans for the regional market in 2022 and beyond?

We will continue growing by doing what we've done: listening to our integrator, distributor and end user patterns; earning and re-earning trust every day; and hiring the best technical and business staff that suit ISS's honest, innovative and team-oriented culture.





asswords were created as a security measure to help keep information secure. Over the years, they have ranged from basic words to complex number-symbol-alphabet combinations. However, most of us take our passwords for granted, considering them as a gateway to access personal information online.

But how relevant are passwords today? Considering that hacking is becoming more and more sophisticated today and that technology has introduced much more strong and in-depth defence mechanisms that easily outshine the age-old password, isn't it time we replaced it with something more futuristic?

According to Bernard
Montel, Technical Director and
Cybersecurity Strategist at Tenable,
"When World Password Day began
[in 2013,] its emphasis was on
encouraging users to create and use
strong unique passwords. Given the
number of data breaches reported,



ANTOUN BEYROUTHY
LEAD CYBERSECURITY CONSULTANT AT AXON
TECHNOLOGIES



APARNA RAYASAM
CHIFF PRODUCT OFFICER AT TRELLIX



BAHAA HUDAIRI
REGIONAL SALES DIRECTOR META AT

where scammers have obtained a database of username and passwords, creating the strongest password in the world isn't going to help if scammers already know it."

In his opinion, it's "frightening" that we're still protecting digital identities solely with an email address and password combination in 2022. "And when it comes to non-human service accounts, that often have administrative access to core databases and applications, the use of passwords is still common practice," he adds.

The problem with passwords is that most of us think of it as fool-proof and 'enough' to protect our online data. What we don't realise is that it takes hackers mere minutes to tear into those passwords and access all the information we thought was safe. In fact, it's alarming that despite the advent of Multi-Factor Authentication (MFA) and other tools [that don't solely rely on passwords], far too many online services still won't enforce these additional measures. There is also an argument when implementing MFA, to strengthen this by using a strong Privileged Account Management tool, implementing policies that require least use privilege for all accounts, strong auditing for all service accounts, and limiting the applications and data that can be accessed.

Aparna Rayasam, Chief Product Officer at Trellix, says passwords are at most "weak" defences and certainly shouldn't be a primary counter measure against the growing range of cyber-attacks.

"Security practices have moved on and multifactor authentication (MFA) is now commonplace, with biometric information increasingly being used to thwart attacks. That being said, the use of passwords persists and it's critical THE PROBLEM WITH PASSWORDS IS THAT MOST OF US THINK OF THEM AS FOOL-PROOF AND ENOUGH TO PROTECT OUR ONLINE DATA. WHAT WE DON'T REALISE IS THAT IT TAKES HACKERS MERE MINUTES TO ACCESS THAT INFORMATION.

for organisations of all sizes and sectors to educate employees on best practices for password management."

Sam Curry, Chief Security Officer at Cybereason, concurs. "My advice to companies is to instruct employees not to trust passwords and use additional factors in all accounts and services. In addition, password managers are a useful tool that can improve password security and management. However, they exist as a compromise due to the failings of passwords themselves."

So then, it's amply clear that the time has come to junk the password habit. However, in a world where passwords are still the norm, how do we ensure that our passwords are strong enough to withstand cyber assaults?

MFA TO THE RESCUE

Hadi Jaafarawi, Managing Director - Middle East at Qualys, has a solution to the password problem. "In today's world, passwords alone are not enough to keep IT access secure. As such, tools like multi-factor authentication [MFA] - which require users to provide two or more verification factors to gain

access to a resource - have become available to further improve security hygiene. Companies, no matter the industry or size, must recognise the value of strong security and doing the small things, like implementing MFA right," he suggests.

So, what can companies be doing to improve password hygiene? "For starters," he says, "ensure that users cannot use a simple dictionary word as their password, and enforce different controls so they cannot re-use the same password multiple times. It is important to apply rules on length of passwords and the variety of characters used, in addition to looking out for poor security practices such as missing MFA or lack of role-based access control."

Toni El Inati - RVP Sales, META & CEE at Barracuda Networks points out that despite significant awareness, employees still utilise weak passwords so user training needs to go hand-in-hand with tools and policies. "Password management is a critical first step, but it's not enough. Companies need to deploy

TOOLS SUCH AS
MULTI-FACTOR
AUTHENTICATION
WHICH REQUIRE
USERS TO PROVIDE
TWO OR MORE
VERIFICATION
FACTORS TO GAIN
ACCESS TO A
RESOURCE-HAVE
BECOME AVAILABLE
TO FURTHER IMPROVE
SECURITY HYGIENE.

anti-phishing protection as well as the right application and edge security solutions. Passwords aren't going away anytime soon, and the with 80% of all basic web application attacks still relying on stolen credentials, neither are attacks."

Bahaa Hudairi, Regional Sales Director META at Lookout puts it differently. "The best thing to do to highlight the importance of strong passwords is to make people understand the value of the data that these passwords are supposed to protect," he says.

"Consumers tend to assume that the services where they upload and share this sensitive information will protect them, but in reality the best line of defence is at the point of the consumers themselves. People should be educated about enabling multifactor authentication, wherever possible, as an absolute must. This provides a second layer of defence in the event that the attacker is able to get your password," he goes on to add.

More important than all of these is perhaps, the most commonly committed, yet underestimated, password-related error: Using the same ID/email address and password across multiple sites and devices. "Password reuse is exacerbated by the increasing volume and success rates threat actors are reaping with advanced credential phishing campaigns that use fake websites resembling the login page of a legitimate online service to steal usernames and passwords," says Emile Abou Saleh, Regional Director, Middle East and Africa at Proofpoint.

"We recommend consumers use different passwords, especially on critical financial and data-driven accounts. Be sure to turn on multifactor authentication (MFA) if available



BERNARD MONTEL
TECHNICAL DIRECTOR AND CYBERSECURITY
STRATEGIST AT TENABLE



EMILE ABOU SALEHREGIONAL DIRECTOR, MIDDLE EAST AND
AFRICA AT PROOFPOINT



HADI JAAFARAWI MANAGING DIRECTOR - MIDDLE EAST AT OLIALYS



LANCE SPITZNER
SENIOR INSTRUCTOR & EXPERT IN HUMAN RISK
AND SECURITY AWARENESS AT SANS INSTITUTE



SAM CURRY
CHIEF SECURITY OFFICER AT CYBERFASON



TONI EL INATI
RVP SALES, META & CEE AT BARRACUDA
NETWORKS

for as many accounts as possible," he adds. "If MFA is not an option for the account, use a password manager. A password manager creates randomised passwords that are safely stored, encrypted, and accessible across all personal devices and reduces the burden of trying to remember complicated login credentials across multiple websites. If you use a passphrase as part of your password, make sure you never use common words or phrases, names or dates associated with you or direct family members. It's also best to change all passwords twice a year and change business passwords every three months."

Managing passwords is not an easy task, says Antoun Beyrouthy, Lead Cybersecurity Consultant at Axon Technologies." Avoiding reuse and utilising complex passwords makes memorising passwords nearly impossible. Individuals are therefore advised to use password managers which generate and store complex passwords when registering for a service. The password is then automatically submitted at each log on."

"On the other hand, businesses are advised to deploy an Identity and Access Management solution, enabling single sign-on and centralised access management capabilities. Employees no longer need to remember multiple passwords, administrators have more control over accounts and privileges, and auditors can pull all user access information from a single source," he adds.

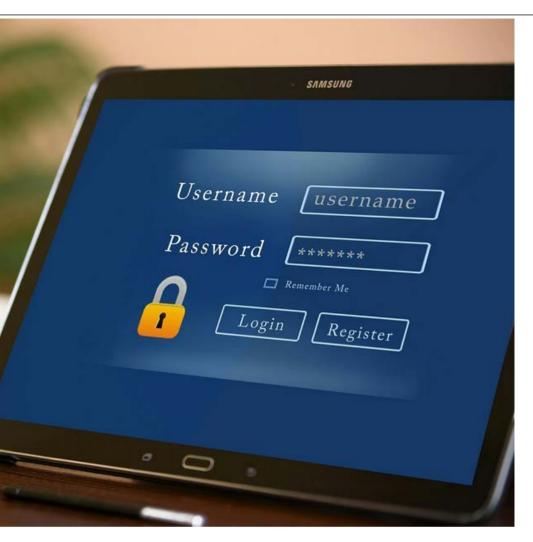
Then again, he says, there might be challenges when integrating with legacy systems, so businesses need to ensure their IAM solution provides the customisability required for such integrations. "Finally, whether you are an individual or a business, always



make sure that you are using multifactor authentication, at least for critical services and applications."

Lance Spitzner, Senior Instructor and expert in Human Risk and Security Awareness at SANS Institute, vouches for Multifactor Authentication (MFA) as a strong authentication method.

"One of the most effective and proven approaches for strong authentication is something called Multi-Factor Authentication or MFA for short. MFA is when multiple factors of authentication are used. That way, if your password is compromised, your account, system, or data is still safe as the other factor, or factors, still protect you. MFA is becoming a popular solution, but there can be a great deal of confusion on exactly how MFA works as well as the different implementations of it."



MANAGING
PASSWORDS
IS NOT AN EASY
TASK. AVOIDING
REUSE AND
UTILISING COMPLEX
PASSWORDS
MAKES MEMORISING
PASSWORDS
NEARLY IMPOSSIBLE.
INDIVIDUALS ARE
THEREFORE ADVISED
TO USE PASSWORD
MANAGERS.

In fact, Microsoft estimates that MFA defeats 99% of authenticationbased attacks. While not fool-proof, MFA is one of the most effective steps organisations can take to dramatically reduce the risk of a breach. At its simplest level, MFA is multiple levels of authentication. An individual authenticates not only with a password (something they know), but some type of unique code or device they have. Even if their password is compromised, their account, or data, is still safe as the cyber attacker does not have access to the second form of authentication. Unfortunately, that is where the simplicity of MFA stops and things can get a bit complicated.

There are many different terms to describe MFA (Multi-Factor Authentication). Some organisations or vendors call it Two-Step Verification, Two-Factor Authentication (2FA), One-Time Password (OTP), or Strong Authentication. All are implying the same thing, authentication requiring two or even more forms of authentication, usually a password and something else – often a unique code sent to, or generated by, your mobile device.

In addition, there are multiple ways to implement MFA. Some of the most common methods are listed below. This list is by no means exhaustive. It merely highlights the most common.

SMS Code: A one-time, unique code is sent to your mobile device. You then use this code in addition with your password to authenticate and login. This is the most commonly used approach as it is the easiest to setup.

Code Generator: Your mobile device has an authentication mobile app (such as Google Authenticator) that generates the unique one-time codes for you. You download the mobile app to your mobile device, then to enable MFA for your accounts you synch the authentication app with each account. These authentication apps can support hundreds of accounts at the same time.

FIDO: You are given a physical device that connects to your laptop or computer. This physical device is registered with the websites you regularly log into. This physical device than must be connected to your computer (such as inserted into the USB port or connected via NFC technology) and authenticates you. Yubikey is a common, publicly available example of such a physical device supporting the FIDO standard. This approach is considered to be the most secure method of authentication, as there is no unique code or authentication request, there is nothing for cyber attackers to trick or fool their victims out of.



igital transformation has been a key enabler of Saudi Vision 2030 which aims to diversify the Kingdom's economy, while promoting new industries. Ever since, Saudi Arabia intensified its steps towards becoming one of the leading countries to power the Middle East's digital transformation scene. According to IDC, Saudi Arabia's ICT spending is expected to reach \$32.9 billion in 2022, a year-on-year growth of 2.3 percent.

However, security has become inseparable from digital transformation; and, with the rise of digitisation in Saudi Arabia, it has become a target for cyber criminals.

As cyberattacks continue to grow in both volume and complexity, cyber

security must be front of mind for all organisations. Accordingly, in 2017, Saudi Arabia established National Cybersecurity Authority (NCA), with the mission to strengthen and enhance the kingdom's cybersecurity infrastructure and to develop policies, governance mechanisms, standards, controls and guidelines.

Is hybrid cloud the answer to cybersecurity?

Many CIOs are too focused on short term security solutions, relying on cloud as a safety net and overlooking their longer-term cyber resilience strategy. So, why isn't a hybrid cloud strategy enough to ensure cyber resilience, and what can organisations Saudi Arabia and the region do to bake in resilience by design?

CIOs spend a huge amount of time, money, and resources on cloud strategies, and their decisions can have significant repercussions across the entire business, for staff and customers alike. However, the way departments often purchase and utilise cloud resources can significantly undermine a business's overall level of resilience.

What do we mean by resilience?

It is vitally important for the majority of companies that they are able to continue their operations around the clock.

On recent years, severe outages and cyberattacks have driven headlines that have significantly damaged the reputation and revenue of affected organisations, on top of interrupting their ability to serve their customers. Central to this "always-



kyndryl.

requires a breaking of this mould: a fundamental rethink of how we design, procure, and maintain our systems with business operations in mind, and data's central role within this.

Adopting a resilience-first mindset

Today, at a time where disruptions must be expected, CIOs are butting heads with their own enterprise architectures and processes, coming to the realisation that the model they've been using for the last 30 years is no longer viable. The IT industry has compartmentalised itself into neat towers and silos, evolving into, and being sold as, individual dedicated disciplines. These fragmented disciplines do not in turn correlate to end-to-end business functions.

This siloed approach is particularly unhelpful in the event of a cyberattack. For example, whose job is it to find a solution when an attacker brings down a network and customer information is lost? SecOps? Disaster recovery? Network? Datacentre? These towers create responsibility gaps which make it impossible to mount an effective response.

THE WAY
DEPARTMENTS
OFTEN PURCHASE
AND UTILISE CLOUD
RESOURCES CAN
SIGNIFICANTLY
UNDERMINE A
BUSINESS'S OVERALL
LEVEL OF RESILIENCE.

Building a resilience framework within your cloud strategy Cyberattacks or network outages can

Cyberattacks or network outages can ripple through multiple departments within an enterprise and following the breadcrumbs of a system failure to its root cause can feel like relay race between teams. Time is not the only currency spent in the race to find the source of a breach, either: those delays also mean significant financial and reputational losses.

Changing the existing cloud model is a hugely complex ask, extending beyond an organisation's tech stack to the wider business. The more manageable approach, therefore, is to develop a resilience framework, consisting of step-by-step processes, requirements, and considerations to bring IT towers into a more cohesive alignment. The challenges lie in both developing an exhaustive resilience framework in the first place, and then actively retrofitting it to your existing tech stack and internal operations.

Enabling true resilience

The data journey is the Achilles heel of any hybrid-cloud strategy. The way that it flows, how discoverable it is, its quality and usability, and, ultimately, who's in charge of getting it up and running again in the event of an outage or a cyberattack. Proper resilience practice is not about knowing who to hand off to in an emergency – it's truly knowing how your system fits together.

To break down silos and effect true change, then, CIOs need to understand their minimum viable organisation and their risk appetites so that they can invest and act appropriately. Without an effective resilience strategy, any hybrid cloud strategy risks grinding to a halt. 1

on" service demand is data; ensuring that it is always available, reliable, secure, and has an immediately available back-up environment available if its primary environment goes down.

Current Enterprise IT architecture is not built to think in terms of business operations. Questions like "Can my doctors access medical data? Can my bank access money? Can my users reach my content?" don't mean a lot to technology towers like networking, data centres, security, or cloud operations in isolation – yet each are a vital link in the process chain.

The technology industry has institutionalised itself into these competing towers, often to the detriment of business operations and resilience. Achieving proper resilience, therefore,



LUXURY HOTEL IMPLEMENTS STATE-OF-THE ART SURVEILLANCE SYSTEM WITH SUPPORT OF SEAGATE DATA STORAGE SOLUTIONS



afety and security in tourist capital, Dubai
While the city of Dubai is touted as one of the safest in the world, the city is home to many iconic buildings and properties, which are visited by millions of people every year. As such, for responsible building operators, security must be a priority. Indeed, the attention paid to security enables the city to maintain its reputation for safety that keeps tourists coming back.

Despite Dubai's high level of safety, Downtown Dubai, home to the Burj Khalifa, the world's tallest building, Dubai Mall, the world's largest shopping mall, and a luxury hotel, a popular tourist destination, is glittering envy of the world. With 16.73 million people visiting Dubai in 2019 and Downtown Dubai, one of the city's most popular areas, it is imperative that building operators can keep track of who and what is going on at their sites 24/7.

Upgrading the Luxury Hotel's outdated surveillance system

With that said, it should come as little surprise that a luxury hotel in Downtown Dubai, which is divided

into two parts- hotel rooms and residential apartments, features over 1,500 cameras across its facility to protect its visitors, staff, and building. The luxury hotel is owned and operated by the Abu Dhabi National Hotel (ADNH) and Residences is by Emaar Hospitality. However, the hotel's security system, which was previously unified by one unified video surveillance system, recently became outdated and was no longer compliant with existing regulations and had an expired warranty. With these ongoing operational and running issues of both the hotel and residences, operators of a luxury hotel in Downtown Dubai contracted Dubai-based company Agility Grid to install an innovative video surveillance and analytics solution to replace its outdated security system and both companies mutually agreed to separate the video surveillance. This led to the Seagate storage to be deployed in the hotel as a part of the SIRA compliance, which included recording at certain parameters.

However, installing a brand-new surveillance system is a little more complex than replacing old cameras with new ones. Unlike their older analogue counterparts, digital video surveillance must be supported with sufficient storage space to enable their full and effective functionality. This was especially true for a luxury hotel in Downtown Dubai because not only was a storage expansion required, but also both systems were also upgraded to the latest Milestone XProtect version to comply with

Video Guard requirements. Indeed, robust storage infrastructure is essential to switch to the innovative video surveillance system where video streams would be of highest resolution, recorded for a longer period to enable all insights and analytics. Storage infrastructure and its capacity will essentially determine the number and duration of each video stream, the image quality in terms of resolution and frames per second, and for how long each video stream would be stored. In the case of a building such as the luxury hotel. high-quality video streams, with the highest resolutions and maximum frames per second, are important to be on the top of suspicious or dangerous activity in the area. But this requires a more substantial storage solution.

The Seagate Exos 2U12 solution

Agility Grid approached the Seagate enterprise solutions team with the request to develop a tailormade storage solution for a luxury hotel in Downtown Dubai's' security needs. Following a proof of concept, the Seagate Exos 2U12 storage solution, a 2U rackmount enclosure unit, was adopted. This Exos solution offers a versatile, space-saving storage building block that is efficient, agile, and scalable. With flexible capabilities to support cables, universal ports, configuration controls, and standard zoning, the components on the modular system are interchangeable

SEAGATE IS
LOOKING FORWARD
TO WORKING WITH
FUTURE PARTNERS
TO BOOST AND
OPTIMISE STORAGE
CAPACITY TO
ENABLE A NEW ERA
OF SURVEILLANCE.

for optimal data availability. Finally, cost-efficient and with energy-efficient features, the solution is well suited to high-capacity environments. Offering exceptional performance and less risk of downtime, Exos 2U12 provides a luxury hotel in Downtown Dubai's operators peace of mind that their video surveillance system will operate to maximum capacity, offering its visitors optimum security.

Final thoughts

Offering the most innovative and easily integrating storage services built on trust, affordability, and performance, working with a luxury hotel in Downtown Dubai and Agility Grid demonstrated that Seagate continues to deliver a seamless experience at the best value. The company is looking forward to working with future partners to boost and optimise storage capacity to enable a new era of surveillance where second-to-none image quality, archival needs, and the latest features such as facial recognition are taken into consideration. In doing so, our solutions enable governments, businesses, and building operators to quarantee the highest possible levels of safety for their citizens, customers, employees, and the general public.

regardless of size or budget, making the unit easy to set up, maintain and expand. Moreover, the solution safeguards data thanks to intelligent fault diagnosis, persistent error logging, and monitoring. It is 95% faster than those solutions reliant on low-cost, low-capacity hard disk drives (HDD), often used to minimise storage expenses. Offering speeds of up to 14.4 GB/s in a single I/O module or 28.8 GB/s in a dual controller configuration, the Exos 2U12 storage solution is ideal for high-capacity and transaction-dependent environments that demand faster response times





E: info@linkshadow.com | T: +1 877 267 7313 | W: linkshadow.com

DIGITAL FIRST **APPROACH**

CNME EDITOR MARK FORKER MODERATED A ROUNDTABLE DISCUSSION BETWEEN DELL TECHNOLOGIES & INTERTEC SYSTEMS. WHICH EXAMINED THE IMPORTANCE OF NEXT-GEN CLOUD INFRASTRUCTURE IN THE DIGITAL ECONOMY. HOW BUSINESSES CAN RECOVER THEIR MISSION CRITICAL DATA FOLLOWING A CYBERATTACK - AND HOW ENTERPRISES CAN ADD 'VALUE' TO THEIR AGILE INFRASTRUCTURE



ell Technologies are one of the most innovative technology companies in the world, but they are an organisation that does not rest on their laurels.

Innovation is infused in their DNA, and they are constantly investing in R&D to develop solutions and technologies to address the customer demands of today's complex IT ecosystem.

Intertec Systems is one of the most respected systems integrators in the UAE and has been in business for over 30 years.

During that time, it has earned a reputation for being one of the most reliable and trusted IT service specialists in the region, evidenced by the close relationship it enjoys as a channel partner of Dell Technologies.

In what was an extremely informative, engaging, and thoughtprovoking roundtable discussion, the session was kickstarted by Bassam Zantout, Enterprise Architect at Dell

Technologies in a session entitled 'Infrastructure for Cloud-Native Platforms'

In what was a fascinating presentation, Zantout highlighted how application modernisation was a huge challenge with business and technology teams being misaligned.

"We know that application modernisation enables organisations to make the most of their digital technologies, whether it be AI, machine learning, big data, and cloud. It helps transform your IT ecosystem based on current market trends and build a

CLOUD-NATIVE APPLICATIONS ARE THE FUTURE OF SOFTWARE DEVELOPMENT

flexible foundation for future innovation. However, we know that far too many enterprises are taking an API-only approach to app modernisation and some vendors are quilty of overcharging customers looking for application modernisation," said Zantout.

Zantout said that unlike other vendors, Dell Technologies supported choice and advocated for the use of Kubernetes for managing containerised applications across multiple hosts.

"Cloud-native applications are the future of software development. Exploiting the advantages of the cloud computing delivery model, a cloudnative application offers greater agility, resilience, and portability across public, private and edge cloud environments. Cloud With Dell Technologies Cloud, enterprises can deploy a hybrid cloud model and run traditional workloads alongside cloudnative, container-based applications, managing everything from a single pane of glass," said Zantout.



The next presentation was conducted by Ashraf Helmy, Regional Channel Sales Manager at Dell EMC, who showed the methods and solutions businesses can deploy to help them recover from the devastating impact of a cyberattack.

Cyberattacks as we all know are on the increase and are becoming more sophisticated, meaning that they can be harder to detect, flag and prevent.

Helmy made no qualms when it declared that businesses need to understand that it is not a case of if we will be attacked, but instead when.

"We are seeing more and more cyberattacks every day, and there has been an exponential increase since the onset of the COVID-19 pandemic. But what is your plan as a business? Too many enterprises are guilty of thinking it's not going to be them, why would they attack me? But research has shown that 49% of those attacked are SMEs, many of whom are left crippled if they need to pay a ransomware fee to get their

data back. That statistic shows you that these cybercriminals are not just going after the multinational conglomerates, everybody is a target. What businesses need to understand is how they can mitigate the damage of an attack when they are hit," said Helmy.

In addition to this, Helmy also pointed out that an employees' PC was the weakest part of the security chain, and this was a major issue facing large organisations in a hybrid world.

"We now live in a work from anywhere world, but that has made employees in many cases sitting ducks. They are vulnerable, and we have seen countless cyberattacks via this method. The PC is the weakest part of the chain, and it's important for enterprises to recognize that a disaster recovery plan is very different to cyber recovery, as I stated earlier, businesses need to start thinking about when they are attacked as opposed to if and have a concrete plan in place to mitigate and offset the damage done," said Helmy.

The final session of the roundtable discussion was conducted by Manish Uttpal, Senior Presales Consultant at Intertec Systems, who delivered a presentation called 'Adding Value to your Agile Infrastructure'.

He gave a detailed overview of the company's impressive track record in the region since its inception in 1991 and spoke about its converged infrastructure.

"Our converged system for virtualisation can be managed with a common management platform across servers, storage, and networking. Automation capabilities and templates are in place to eliminate many manual operations and device-focused processes. Vendor support is available to help prevent problems through continuous scanning, dashboard reporting, personalised consultation, resolving issues faster and making system-level updates easier," said Uttpal. 1

A LOSING BATTLE?

DANNY ALLAN, CTO & **CLAUDE SCHUCK,** REGIONAL DIRECTOR, MIDDLE EAST AT VEEAM, TELL SECURITY ADVISOR ABOUT THE FINDINGS OF THE RANSOMWARE TRENDS REPORT WHICH REVEAL THAT BUSINESSES ARE LOSING THE BATTLE WHEN IT COMES TO DEFENDING AGAINST RANSOMWARE ATTACKS

ansomware has democratised data theft and requires a collaborative doubling down from organisations across every industry to maximise their ability to remediate and recover without paying the ransom," said Danny Allan, CTO at Veeam. "Paying cybercriminals to restore data is not a data protection strategy. There is no guarantee of recovering data, the risks of reputational damage and loss of customer confidence are high, and most importantly, this feeds a self-fulfilling prophecy that rewards criminal activity."

According to the Veeam 2022
Ransomware Trends Report,
businesses are losing the battle
when it comes to defending against
ransomware attacks. It found that 72%
of organisations had partial or complete
attacks on their backup repositories,
dramatically impacting the ability
to recover data without paying the
ransom. Veeam Software, the leader in
backup, recovery and data management
solutions that deliver Modern Data
Protection, found that 80% of successful
attacks targeted known vulnerabilities
— reinforcing the importance of

patching and upgrading software. Almost all attackers attempted to destroy backup repositories to disable the victim's ability to recover without paying the ransom.

"One of the hallmarks of a strong Modern Data Protection strategy is a commitment to a clear policy that the organisation will never pay the ransom, but do everything in its power to prevent, remediate and recover from attacks," added Allan. "Despite the pervasive and inevitable threat of ransomware, the narrative that businesses are helpless in the face of it is not an accurate one. Educate employees and ensure they practice impeccable digital hygiene; regularly conduct rigorous tests of your data protection solutions and protocols; and create detailed business continuity plans that prepare key stakeholders for worst-case scenarios."

The Veeam 2022 Ransomware Trends Report reveals the results of an independent research firm that surveyed 1,000 IT leaders whose organisations had been successfully attacked by ransomware at least once during the past 12 months, making it one of the largest reports of its kind. The first of its kind study examines the

key learnings from these incidents, their impact on IT environments and the steps taken to implement Modern Data Protection strategies that ensure business continuity moving forward. The research project specifically surveyed four IT personas (CISOs, Security Professionals, Backup Administrators and IT Operations) to understand cyber-preparedness alignment across organisations.

Of the organisations surveyed, the majority (76%) of cyber-victims paid the ransom to end an attack and recover data. Unfortunately, while 52% paid the ransom and were able to recover data, 24% paid the ransom but were still not able to recover data resulting in a one out of three chance that paying the ransom still leads to no data. It is notable that 19% of organisations did not pay the ransom because they were able to recover their own data. This is what the remaining 81% of cyber-victims must aspire to — recovering data without paying the ransom.

One thing Allan emphasised is that prevention requires diligence from both IT and users, since the "attack surface" for criminals is diverse.

Cyber-villains most often first gained



Danny Allan, CTO at Veeam (L) and Claude Schuck, Regional Director, Middle East at Veeam (R)

access to production environments through errant users clicking malicious links, visiting unsecure websites or engaging with phishing emails — again exposing the avoidable nature of many incidents. After having successfully gained access to the environment, there was very little difference in the infection rates between data center servers, remote office platforms and cloud-hosted servers. In most cases, the intruders took advantage of known vulnerabilities, including common operating systems and hypervisors, as well as NAS platforms and database servers, leaving no stone unturned and exploiting any unpatched or outdated software that they can find. It is notable that significantly higher infection rates were reported by Security Professionals and Backup Administrators, compared with IT operations or CISOs, implying that "those closer to the problem see even more of the issues."

Respondents to the survey confirmed that 94% of attackers attempted to destroy backup repositories and in 72% of cases this strategy was at least partially successful. This removal of an organisation's recovery lifeline is a popular attack strategy as it increases the likelihood that victims

ORGANISATIONS
ARE BEGINNING
TO REALISE THAT
RANSOMWARE
ATTACKS ARE
IN FACT THE
SAME AS A FULLSCALE DISASTER
RECOVERY
SCENARIO

would have no other choice than to pay the ransom. The only way to protect against this scenario is to have at least one immutable or air-gapped tier within the data protection framework — which 95% of those we surveyed stated they now have. In fact, many organisations reported having some level of immutability or air-gap media in more than one tier of their disk, cloud and tape strategy.

"The Middle East is certainly not immune to cyberattacks. The opposite is in fact true. Our region is heavily targeted by sophisticated hackers. Organisations are beginning to realise that ransomware attacks are in fact the same as a full-scale disaster recovery scenario. This has helped them better plan and utilise features which Veeam provides like immutability of backups, ensuring a guaranteed recovery point," said Claude Schuck, Regional Director, Middle East at Veeam.

SECURING THE CONNECTED LANDSCAPE

BASHAR BASHAIREH, MD, MIDDLE EAST & TURKEY, CLOUDFLARE, ON ITS RECENT LAUNCH AND ITS PLANS FOR THE REGION.

ive us an overview of your career in the technology industry
I join Cloudflare with over two decades of experience, mostly in the cybersecurity and software industry, where over the past years I helped global technology providers establish and expand presence and operation in the emerging markets, particularly in the Middle East and Turkey.

Prior to joining Cloudflare, I was the Managing Director and Head of Sales for Emerging Markets at CyberRes, the cybersecurity line of business at MicroFocus, managing the sales and business development across the Middle East, Africa, Brazil, Russia, CIS and CEE. Before that I led StarLink Value Added Distribution as their CEO across a 22 country operation, managing their annual business of close to \$500M. In addition, I held several leadership positions at major technology vendors such as Symantec, BlueCoat, Fortinet and CyberGuard.

What factors prompted you to join as regional head of Cloudflare?

Having worked in the domain of cyber security for more than two decades, I can see that Cloudflare is genuine in its mission of building a better Internet that is THE PARALLEL
INCREASE OF
CYBER THREATS
AND ASSOCIATED
BREACHES, PUTS
CLOUDFLARE IN AN
UNPARALLELED AND
UNIQUE POSITION
TO DELIVER THE
REQUIRED CONTENT
IN A RELIABLE, FAST &
SECURE MANNER.

fast, safe and reliable for everyone. Being part of this journey that touches everyone's life is surely an exciting thing to do.

Having spoken to so many customers in the region, I understand that nowadays more than ever, they need to be able to grow their operations by focusing on their core mission without having to worry about their technology. Cloudflare appears to me as one of the most innovative customer-centric companies in the market. More than just technology, we are on a mission to help to build a fast, reliable and secure Internet for a maximum number of people, businesses,

and public organisations.

Cloudflare also has an exceptional company culture with key values such as diversity, principle, collaboration, innovation and transparency.

Finally, I enjoy the opportunity of launching operations from inception in the region. Building successful teams that can deliver future incremental growth and objectives and supporting our customers is an exciting challenge.

Is the opening of the new office in Dubai Cloudflare's first foray into the Middle East region? And can you give us some details about your intended operations in this region.

Today, Cloudflare's network currently spans over 75 cities in the EMEA region including 16 physical locations in the Middle East and Turkey. Cloudflare first invested in the Middle East in 2015. Now with data centers spanning more than 270 cities in more than 100 countries worldwide, the company continues to grow its presence to be even closer to Internet-connected users everywhere.

Cloudflare has about 30 team members from different functions covering the Middle East. We plan to have a team of approximately 20 people working in Dubai by the end of 2022 and are currently planning to grow that number to over 30 by the end of 2023. We are hiring!



What are the opportunities that you see for Cloudflare in the region?

Cloudflare has been associated with delivering fast content over cloud in a most reliable and secure manner, accounting for at least 20% of the global Internet traffic. Cloudflare can cater for and support all types of organisations (businesses and public sector) including those with a social mission. The Middle East and Turkey as an emerging market is characterised by a relatively young population, with 70% of it being under the age of 30. This dynamic youth segment has an insatiable demand for both content and knowledge. To that extent, there has been a rapid uptake in Internet use, and digital transformation initiatives have significantly accelerated over the past couple of years. This trend represents an opportunity for Cloudflare to add considerable value to regional enterprises and in doing so, increase its footprint and market share.

In addition, the region made up of 13 countries with fast-growing and innovation-driven economies presents a unique growth opportunity for Cloudflare to tap into. I can confidently say that this market is at the forefront of technology and early adopters of disruptive technologies such as cloud on a global scale. This is being driven by many factors such as digital transformation where several countries have embraced ambitious programs transforming them into true digital economies. Cloud uptake has accelerated over the past few years in the region and the necessary regulatory frameworks and related compliance policies are now in place to propel enterprises into the next phase of leveraging the benefits of cloud. This transformation is further accelerated as earlier mentioned, by a mostly young and content demanding population-that content being gaming, entertainment, educational, sports or online retail.

The recent pandemic has for sure played a major role in building up this momentum and increasing the urgency in speeding up such a transition.

The parallel increase of cyber threats and associated breaches, puts Cloudflare in an unparalleled and unique position to deliver the required content in a reliable, fast and secure manner to individuals, businesses and public sector alike, elevating the levels of productivity and performance in addition to reducing complexity for users.

To do that, Cloudflare has built a global network and infrastructure across 275 cities around the world with 27 in the MET region, delivering the same connectivity at 50ms performance for more than 95% of customers. The innovation path is stunning. Not only do we provide best in class cyber security solutions with Cloudflare's SASE security platform, Cloudflare One, a Zero Trust network-as-a-service platform that dynamically connects users to enterprise resources, with identity-based security controls delivered close to users. wherever they are, but we also offer an open strong developer platform with Cloudflare Workers.

What are your immediate priorities as regional head?

Over the last two years, Cloudflare has grown its EMEA team by more than 100 percent and counts approximately 700 employees. For the Middle East and Turkey, the initial functions prioritised for the region include launching new data centers, increasing market share by building partnerships, and expanding our customer base.

One of my priorities is to build a successful team through empowering current team members and attracting future talents that would all contribute towards this journey.

www.tahawultech.com JUNE 2022 37

CUSTOMER FIRST

PIERS MORGAN, VP & GM INTERNATIONAL, ESENTIRE, TELLS ANITA JOSEPH ALL ABOUT MDR AND PARTNERSHIP WITH MMA INFOSEC.

here are many organisations
that claim to provide
managed detection and
response cybersecurity
services. How does eSentire
differentiate itself in such a crowded
and confusing market?

We at eSentire are very much at play within the Managed Detection & Response arena-we've been going strong for 20 years and are very, very experienced within the industry. And we have some very unique service capabilities, because we've been working across the globe, detecting threats for those many, many years. We use MDR with a capital "R" and we call it MDR

cubed-Response, Remediation & Results. The most important thing for us is that we deliver results for our customers-in fact, the threat landscape is becoming complex and there is a degree of risk involved for our existing customers and the customers who are coming into to take our services. So we at eSentire, believe ourselves to be the defining company from an MDR perspective, and we say to our customers and our alliance partners that attack on them is attack on us. We take it personally.

There is confusion between MDR and MSSP. A lot of people tend to think of both of the same things. Can you tell us the

difference between these two concepts?

We like to describe ourselves as a specialist MDR Corporation, but we are more of a hybrid technology company. We have our own proprietary Software as a Service that we have developed over the years and continue to develop, which is very much linked to our Atlas XDR platform, which is where I suppose we could say our secret source exists within that platform to service our customers' needs. I think Managed Service Security providers, or MSSPs, as the acronym says, they spread themselves very, very thinly. We concentrate purely on security service-security as a service &



MDR detection and response level. We don't get involved with firewalls or the gateway. We do work with some very, very key alliance partners and have done for many years in terms of our established relationships going to market with them.

Why is the Middle East such an important region for you?

I think the whole globe is a lot smaller place now particularly from a securitythreat-landscape perspective. We see the region as having been always tech savvy, leading edge, but at the same time presenting risks to all of those companies and corporations that are

based here. So what we are doing now at the moment is that we are investing heavily with both our partners through the Alliance program and also taking our value proposition and how we can actually help corporate enterprise customers across a multitude of different verticals and sectors-from healthcare through to finance through to manufacturing through to shipping, oil & gas, government-and we have solutions that we can tailor make to suit our customers' needs. We're not an offthe-shelf organisation. In in terms of the region, we're seeing exponential growth for our own business, but the only reason that is growing is because the companies within this region are also growing and becoming more globally visible and stretching their own wings. So it's a very exciting time here in the Middle East. We're very proud to be part of it. We're at the start of a long and exciting journey but we are looking forward to forging ahead and scaling our capabilities in the coming months and years.

Tell us about your collaboration with MMA InfoSec

MMA were our first exclusive partner that we appointed, very much concentrating on the United Arab Emirates, and they

www.tahawultech.com JUNE 2022 39



are exceeding our expectations. The reason that we chose MMA Infosec is their expertise and knowledge of that whole security fabric, both in the regionhow they are very much forward thinking in terms of understanding the market and the needs of customers. They're very, very knowledgeable both from a technical and a commercial perspective, in terms of actually listening to customers on what they need. There are many, many partners out there that want the eSentire logo or many other security vendor logos, and they will go and dictate and tell the customers. What I like about MMA InfoSec is that they actually sit down and let the customer talk. They ask the CISO and his leadership team: What's keeping you up at night? What are the headaches? Where are you stretched on resources? What can we as best-in-class providers of services help with, to relieve some of that pressure? And maybe let the CISOs sleep better at night?

Tell us a little more about the synergy between the eSentire and MMA Infosec?

If you look at our value proposition, which is very much around response, remediate

and delivering results quickly, MMA has a similar outlook for all of their customers. They are providing solutions, not a revolution. They're not trying to reinvent the wheel, but they are keeping up with technology, particularly within the security environment. And I think that's what attracted us to, as you say the synergy between our own value proposition and their thoughts on their own marketplace where they've been very successful. I think there was just a natural capability and fit. And we also get on very well-we

WE AT ESENTIRE
BELIEVE OURSELVES
TO BE THE DEFINING
COMPANY FROM AN
MDR PERSPECTIVE
AND WE SAY TO OUR
CUSTOMERS AND OUR
ALLIANCE PARTNERS
THAT ATTACK ON THEM
IS ATTACK ON US.

celebrate the wins together, but we also try and understand why we sometimes lose-why that has happened- and then we move on from there. It's been a great journey and we're looking forward to a great future with them.

So it's going be a very exciting future with two very customer-focused organisations.

We're very much about being customercentric and we share that same vision. I've said it once or several times and I will say it again-it's about listening to and understanding the frustrations that the customer has, but also acting as that trusted adviser. And when it's very easy for me to say what is your headaches, what's keeping you up at night? But also, if you look at how we go to market and how our various business areas work within the center, from our operations team, through our customer success managers through to our network specialists to through to our threat response unit who act within minutes on any threats to our customers. Then, MMA are also there to basically hold our hands in front of the customer and make sure we deliver those results with a capital R.

zendesk

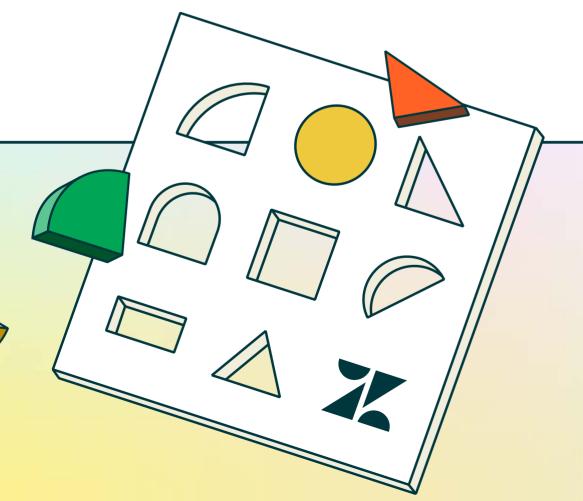
INTERACTIVE REPORT

CX Trends 2022

Access the latest research in our interactive report









enable Holdings, Inc, the
Cyber Exposure company, has
announced it has closed its
acquisition of Bit Discovery,
Inc. ("Bit Discovery"), a leader
in external attack surface management
(EASM). Tenable will launch Tenable.
asm, a new solution that will provide
the full capabilities of Bit Discovery's
technology and enable customers to gain
a more complete 360-degree view of
their full attack surface so they can better
understand how attackers could gain
access via the internet and help prioritise
remediation steps.

Gaining Visibility Into Unseen Risk

An organisation's digital footprint extends far beyond its walls as various services, applications and APIs are internet facing or reside on the internet. To avoid new points of security vulnerability and to ensure good organisational risk management, it is critical for organisations to have visibility into and to understand both known and previously unknown internet-facing assets.

Modern organisations require continuous monitoring of their complete attack surface and context-aware intelligence on where to prioritise remediation efforts. Tenable.asm will continuously map the entire internet and discover connections to an organisation's internet-facing assets, whether internal or

external to their networks, to assess the security posture of their entire external attack surface. When used with the rest of Tenable's solutions, customers will be able to get the context of potential attack paths from external systems to critical assets throughout their organisation providing a comprehensive measure of their overall exposure. Tenable.asm is scheduled to be available for purchase early in the third quarter of 2022.

Because the security of internet-facing assets is a top CISO priority and pain point, Tenable is also integrating foundational quarterly attack surface discovery into its existing market-leading cyber exposure solutions at no additional cost to Tenable customers. New capabilities are scheduled to be included in Tenable.io®, Tenable.

TENABLE.ASM WILL
CONTINUOUSLY MAP THE
INTERNET & DISCOVER
CONNECTIONS TO
AN ORGANISATION'S
INTERNET-FACING
ASSETS, WHETHER
INTERNAL OR EXTERNAL
TO THEIR NETWORKS.

sc[™]and Tenable.ep[™] early in the third quarter of 2022. A new version of Nessus will also include asset discovery.

"Very few, if any, organisations truly understand their full digital footprint. One of the most common but dangerous security lapses is to misconfigure something in the cloud and make it internet-facing. Organisations increasingly have less of a grasp on which of their assets are exposed," said Glen Pendley, Chief Technology Officer, Tenable. "Every business or government entity should have advanced capabilities like those found in Tenable.asm, but given the critical security importance of having ASM everywhere, Tenable is making sure that its customers have at least foundational discovery functionality within the solutions they're already using. This will enable them to spot points of vulnerability that have been completely invisible until now, with the goal of preventing attacks rather than simply managing them."

Bit Discovery provides Tenable customers with:

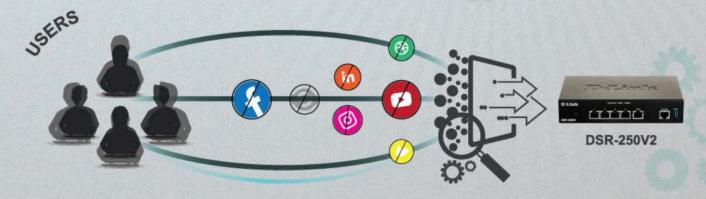
- Discovery of previously unknown internet-connected assets
- Rich context and attribution for domains, sub-domains and other exposed technologies
- Continuous monitoring of the constantly changing external attack surface.

Secure, High-performance NETWORKING VPN SOLUTION

Unified Services Router



IMPROVED Application Control



The DSR-250V2 uses application control to help accurately shape network traffic by either giving priority or applying control policies to effectively manage network utilization. Using packet inspection and a database of application signatures based on the application's network usage patterns, the DSR-250V2 gives complete control over the content that is delivered to end users.

Product Highlights

Comprehensive Management Solution

Advanced features such as WAN failover, load balancing and an integrated firewall make this a reliable, secure and flexible way to manage your network

Complete VPN Features

Complete VPN features, as well as IPSec Hub and Spoke technology, ensures secure communication between mobile employees and offices.

Web Authentication Capabilities

Captive Portal allows employees and guest users to be easily authenticated and authorized by accessing customized landing pages





hy is XDR so important today and how does it fit into the whole cybersecurity paradigm?

When we think about

XDR, we need to go back to thinking about what is the outcome, because there are new technologies emerging every day. The outcome is an impact on a KPI called Mean Time To Respond (MTTR). We know that attackers are targeting enterprise organisations. One of the ways to reduce the risk is to be able to reduce the time that it takes organisations to find and stop these attackers. Now a lot of things play into that MTTR — there's visibility, there's detection, there's response capabilities, there's talent, there are processes, but that is the key outcome — how do we reduce the Mean Time to Respond to the incidents? in order to reduce the time to respond, we need to first and foremost see what is happening in our networks and understand when an attack is happening.

In the past, there were two strategies that

were built to try to do that, and both didn't really work that well. Number one was detection capabilities that were focused on a silo in the architecture. So for example, detection in the identity, that would find compromised identities, stolen accounts and these type of things. There was detection on the endpoint to find bad things happening on people's workstations or servers. There was detection on cloud platforms. These were siloed detection capabilities. The problem with that was that attackers often behave like legitimate users in the network. And if you're only looking at one silo? The logs coming from the cloud, or the logs coming from the endpoint, it may not be indicative enough — it may look very, very similar to what a legitimate user is doing, because that's what attackers are doing. They're stealing someone's account and they're behaving like an internal administrator or an internal user. And so the siloed detection controls really failed in finding the more advanced threats, those attackers that know how to evade detection very well. So we knew that we need

to bring in all that data from all these different silos into one place where we can find those behaviours — those more complex behaviours that we can use to detect an adversary. And then came in the SIEM, which is essentially a data lake where you would put all the logs from all these different sources and have all that data in one place.

The problem with a SIEM is that it is a data repository. It's a place to put data in, but it really doesn't produce anything from that data. It's a human being that needs to go through all that data to figure something out. And that doesn't help us get to the outcome of reducing the time to respond because a human isn't really capable of going through all that data, especially in an enterprise environment.

And so in comes the XDR which is about not only bringing in all that data from all those different places in the enterprise and making sure that we have visibility into everything that is happening across the enterprise, endpoint, cloud, identity and access in one place, but also being able to drive automation — automation in analysing

the data, detecting the threat in as close to real time as possible. And understanding what needs to be done to mitigate the risk and then carry out those response actions. So, XDR is really about breaking the detection silos, so we can see the more advanced attacker behaviours in our networks and automate the process of understanding that data and take action on that data so we can reduce that Mean Time to Respond.

What are some of the main XDR trends today?

I would say that there are probably three main trends in the XDR market today. First and foremost is the strength of analytics. If we remember what the outcome that we're trying to achieve is, which is reducing MTTR. and we remember the problem that we had with the SIEM, which is the data sitting in a storage, but doesn't mean anything. Strength of analytics is about to what extent we can automate the process of making sense of that data? Understanding what is happening in our environment in an automated way, detecting threats automatically across our different technologies in our architecture, and understanding what is the response that's needed to reduce the risk or to remove the attacker from the network. And so that's the strengths of analytics. XDR vendors today, that's one factor that they can be ranked on. Vendors that are still very much just data repositories, versus vendors that automate a very large portion of the process. That's the strength of analytics and that's one key trend in XDR.

The second key trend in XDR is the openness of the architecture. In an enterprise environment, there's a very, very large variety of security and IT technologies - cloud technologies on prem technologies, network technologies, identity technologies, endpoint technologies. And so the more data your XDR can take in, the more you integrate, the more you're open to the various components in the enterprise environment, the more capable you are to detect and stop a threat. So there are vendors in the XDR space that are very locked into their own technologies. As opposed to that there are vendors that are very open in their XDR architecture. There's just you willing to take in data from any vendor in the in the IT and in the XDR market today.

The third key trend, talks about how data is important. We need to see everything that is happening in the enterprise environment. What that means is that we need to be able to take in data from, in an ideal world. every enterprise technology, every security technology that exists in an enterprise environment. Most vendors are on that journey. Some of them have integrations with 10 different technologies that are in a typical enterprise environment while others would have 20 or 50 or 100. But obviously, the more integrations you have, the more visibility you can get into the enterprise environment. And so the breadth of the platform or the breadth of integration is another key trend that XDR vendors are investing in very, very significantly and is a key factor in the value of a solution for an enterprise organisation.

XDR vs MDR: give us more clarity here and tell us more about Cybereason XDR.

XDR & MDR are essentially complimentary. XDR is the technology platform that helps people drive the outcome, which is reduce Mean Time to Respond. But some organisations prefer to have those people outsourced. And MDR is essentially the outsourcing of this detection and response, people-operated capability, to a partner. The MDR partner will then use technologies like a Cybereason XDR or XDR technologies to help their people drive more efficient outcomes.

For example, if an XDR technology is able to collect data, see the attack in the network,

CYBEREASON OFFERS
A COMPLETE XDR
SOLUTION WITH
A FULL MANAGED
SERVICE OR AN MDR
TO SUPPORT OUR
PARTNERS AND
CUSTOMERS IN THE
REGION.

alert on that attack and determine necessary course of action to mitigate that attack, but you want a human in the loop to review that recommended course of action and decide if that is indeed what they want to do, that person can either be in an organisation's organic SOC or they can be in an outsourced MDR service. So the MDR is essentially the people expertise that a lot of vendors in the space and a lot of channel partners provide.

Cybereason today offers both a complete XDR solution with a full managed service or an MDR to support our partners and customers in the region. Another interesting aspect of MDR, that I think XDR helps drive, is Incident Response. In some cases, if an attacker is able to get into the network. enterprises would like to sort of raise a red flag and do something called an incident response which is a deeper analysis of what happened. For example, think about a ransomware attack where the attacker was able to impact some of the assets in the network. You'd like to take active action to respond to that to that situation. If you have an effective XDR platform, then the cost of an IR is relatively low because the platform automates the majority of it. If you have traditional technologies, the cost of an IR is fairly high. And so what you see today is how an XDR technology like Cybereason XDR is driving change in the business model of MDR providers, because for example, classical MDR providers that use traditional technologies find an IR project to be extremely expensive. And so enterprise organisations think 10 times before they decide to ask their MDR provider to do an IR, just because it carries a significant expense.

But for a Cybereason MDR partner, as an example, the cost of an IR is very low. And one of the things that we're seeing now is MDRs using a Cybereason offering called an unlimited IR retainer, which basically means that an enterprise organisation can go into Incident Response mode with the partner as many times as they want for the exact same cost, for a fixed cost. The reason is that the cost of a single IR on a platform that automates the majority of it is relatively very low so they can make that change to their business model and be more competitive. \mathbb{1}

www.tahawultech.com JUNE 2022 45

IN 2021, 57% OF ALL CYBERCRIMES WERE SCAMS: GROUP IB



roup-IB, one of the global leaders in cybersecurity. has shared its analysis of the landscape of the most widespread cyber threat in the world: scams. Accounting for 57% of all financially motivated cybercrime, the scam industry is becoming more structured and involves more and more parties divided into hierarchical groups. The number of such groups jumped to a record high of 390, which is 3.5 times more than last year, when the maximum number of active groups was close to 110. The number of brand-impersonating scam resources created per month also increased. In the Middle East and Africa region, Group-IB analysts noted an increase of 150%. This is more than the rise in the APAC region (83%) and Europe (89%). Due to SaaS (Scam-as-a-Service), in 2021 the number of cybercriminals in one scam gang increased 10 times compared to 2020

and now reaches 100. Traffic has become the circulatory system of scam projects: Group-IB researchers emphasise that the number of websites used for purchasing and providing "gray" and illegal traffic and that lure victims into fraudulent schemes has increased by 1.5 times. Scammers are going into 2022 on a new level of scam attack automation: no more non-targeted users. Scammers are now attracting specific groups of victims to increase conversion rates. Social media are more often becoming the first point of contact between scammers and their potential victims.

With more and more Internet users falling victim to cybercrime every day, fraudsters prefer good old techniques such as phishing (18%), scams and fraud (57%), and malware infections and reputational attacks (25%). In 2021, scams were the most common type of cybercrime.

The number of brand-impersonating

scam resources created per month also increased. In the Middle East, Group-IB analysts noted an increase of 150%.

"A strong trend that we observed in 2021 was no-frills scammers merging into groups controlled by highly technically skilled villains," said Antony Dolgalev, Deputy Head of Digital Risk Protection at Group-IB. "Group-IB's Al-based platform identified somewhere between 75 and 110 scam groups last year, and the average number of cybercriminals per group was 10 members. The average number of scam links per group reached 100. SaaS helped grow not only fraudsters' appetites, but also the industry itself. In 2021 our DRP system tracked 350 groups, reaching up to 390 scam groups at the peak time. The number of cybercriminals in fraudulent groups has increased dramatically, averaging between 100 and 1,000 per group. In turn, their infrastructure has grown proportionally: the average number of scam links per group was between 2,000 and 3,000".

The number of websites used for purchasing and providing "gray" and illegal traffic increased by 1.5 times. Scammers refused to create and maintain their own resources. Their task was only to attract traffic to third-party resources owned by other scammers for a fee when the theft of money was successful.

There was no weak URL targeting.
Group-IB experts noted a strong trend towards the use of improved URL targeting: a valid one-off URL, available strictly for a particular user at a specific moment in time, targeted a specific audience. Personalised URLs usually include not only a timestamp and hash, but also geolocation information, the OS version, the browser type, and the name of the Internet provider. There was also no weak content personalisation.
Fraudsters used improved content personalisation with auto-completed web forms on a page with a user's personal data, extracted from browser cookies.



DISPLAY & CONTROL SOLUTIONS WITH PRESENTATION MATRIX & SCALER





Hikvision is the world's leading IoT provider with video as its core competency, commercial display business also being its key focus area. Malco Technologies is an official Hikvision Displays distributor in the UAE, offering LED/LCD Video Walls, digital signage and 3D/transparent screens to suit every Boardroom, Media advertising, NOC/SOC control room requirements. By pairing with Kramer's Matrix switchers, VIA Connect PRO Wireless Collaboration Solution and Video Wall Controller etc. the applications are unlimited.













We Connect You to the World

700+ Global MNO Connections | 40+ Data Centers
24Bn Monthly Transactions | 3500+ Employees
70+ Offices | CPaaS Leader in IDC Marketscape 2021
Rocco Best Customer Engagement Platform 2020
Rocco Best A2P SMS Vendor 2018, 2019, 2020

For more information please visit www.infobip.com