ISSUE 62 | FEBRUARY 2022 WWW.TAHAWULTECH.COM

# SECUL 21

MIDDLE EAST

**HIGHLIGHTS** 

LEVITON THREATQUOTIENT VEFAM

## BUILDING DIGITAL TRUST

HANI NOFAL, VICE PRESIDENT OF GBM DIGITAL INFRASTRUCTURE SOLUTIONS ON THE NEED FOR DIGITAL TRUST TO UNDERPIN THE SECURITY ARCHITECTURE OF ORGANISATIONS.

tahawultech.com

Chine computer news middle east



**WD Purple™** Surveillance Hard Drive **WD Purple™ PRO**Surveillance
Hard Drive

- All Frame Technology
- Western Digital Drive Analytics

#### CONTENTS

#### Security









- News roundup from the cybersecurity landscape in the region.
- Ray Kafity, Vice President Middle East Turkey and Africa (META) at Attivo Networks, on how traditional security solutions are no longer enough.
- Aloysius Cheang, Chief Security Officer at Huawei UAE, on how the company has adopted a secure-by-design philosophy.
- 46 Jermaine Campbell– Head of VIA sales, EMEA at Seagate, on how the company is helping to accelerate digital transformation.



# Be data ready.

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

commvault.com



#### **EDITORIAL**



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

Anita Joseph Editor

#### **EVENTS**





#### **A QUESTION OF TRUST**

As we progress into 2022, the cyber threat landscape keeps getting complex and complicated. Trust becomes integral to every security organisation and customers opt for products and solutions that they think can count on.

Digital trust is even more intricate, because with the acceleration of digital transformation, organisations are leveraging technology to redesign customer and employee engagement, transform operations and adopt new business models to address rapidly changing industry dynamics and user needs. And as organisations reshape themselves to adapt to the expanding digital economy, building resilience and trust into the digital experiences

of customers, employees and partners is becoming increasingly critical.

This is our theme for this issue of your favourite magazine. In an exclusive cover story interview, Hani Nofal, Vice President of GBM Digital Infrastructure Solutions, discusses the need for digital trust to underpin the security architecture of organisations.

But that's not all: Aloysius Cheang, Chief Security Officer at Huawei tells us how the company has adopted a secureby-design philosophy that incorporates cutting-edge security into all of its products and services. Leon Ward, VP of Product Management at ThreatQuotient, says how 2022 will be a busy year for the company as it focuses on bringing to the market an innovative user experience for customers to leverage its approach to automation.

We also have Jermaine Campbell– Head of VIA sales, EMEA at Seagate, describing how the company is helping the market fast track its digital transformation journey with its cuttingedge products and solutions.

That's not all: We even have a special spotlight on Veeam's Data Protection Trends Report 2022 that surveyed more than 3,000 IT decision makers and global enterprises to understand their data protection strategies

for the next 12 months and beyond. The largest of its kind, this study examines how organisations are preparing for the IT challenges they face,

including huge growth in use of cloud services and cloud-native infrastructure, as well as the expanding cyber-attack landscape and the steps they are taking to implement a modern data protection strategy that ensures business continuity.

In addition, we have the regular news roundup and insight columns to help you navigate the cybersecurity landscape easily and seamlessly.

So, this is a power packed issue, one which we hope you'll enjoy and remember. Happy Reading!

FOUNDER, CPI Dominic De Sousa (1959-2015)

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

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com EDITORIAL Editor Mark Forker mark.forker@cpimediagroup.com

OnlineEditor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

PRODUCTION AND DESIGN
Senior Designer
Analou Balbero
analou,balbero@cojimediagroup.com

webmaster@cpimediagroup.com

DIGITAL SERVICES

Web Developer

Adarsh Snehajan

**DIGITAL TRUST IS** 

VITAL FOR ALL-ROUND

SECURITY.

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.

#### **BEYONDTRUST ANNOUNCES RELEASE OF BEYONDTRUST PRIVILEGED REMOTE ACCESS 22.1**



announced the release of BeyondTrust Privileged Remote Access 22.1, which empowers IT/OT teams to control, manage, and audit remote privileged access by authorised employees. contractors, and vendors — without compromising security. Organisations can enforce least privilege, exert granular control and visibility, and layer on advanced credential security over remote access for employees and third parties.

Allowing third-party remote access comes with many potential security risks. Vendors authorised to access the network and applications might not adhere to the organisation's same level of security protocols. They might use weak or default passwords, or share a single set of credentials among multiple individuals. VPN is another risky practice for extending access to third parties, as they are a target for hackers to compromise the supply chain.

To reduce these attack surfaces, BeyondTrust Privileged Remote Access provides greater control over remote vendor access by eliminating "all or nothing" access. All connections are brokered through a single access pathway, with granular, role-based access to specific systems and defined session parameters.

"Third-party vendor remote access is often the weakest link in network and information security," said Daniel DeRosa, Chief Product Officer at BeyondTrust. "We enable organisations to better monitor and manage thirdparty access for privileged users, without inhibiting business agility," he added.

#### HELP AG PARTNERS WITH CYBERARK TO DELIVER **NEW IDENTITY SECURITY SOLUTIONS IN UAE & KSA**

Help AG, the cybersecurity arm of Etisalat Digital and the region's trusted IT security advisor, has introduced an addition to its portfolio aimed at improving security for its customers by focusing on reducing identityrelated risk. With CyberArk, the global identity security leader, Help AG now delivers the most comprehensive Identity Security Platform to its clients in the United Arab Emirates and Saudi Arabia.

Commenting on the partnership, Stephan Berner, Chief Executive Officer at Help AG, said: "Through joining forces with CyberArk, Help AG is demonstrating its commitment to partnering with the world's leading cybersecurity vendors to offer state-of-theart technology platforms to our customers. By adding CyberArk to our suite, we can now offer our customers the most complete and comprehensive identity security offerings to secure identities, both human and machine. This partnership enables us to leverage CyberArk's industry-leading capabilities as we deliver an end-to-end managed service as part of our ongoing mission to









CRAIG HARWOOD

become the region's leading service-centric cybersecurity provider."

Craig Harwood, Regional Sales Director, Africa and Middle East at CyberArk added: "Working with Help AG will further expand the reach of our identity security solutions with customers in this growing region. In serious cybersecurity attacks worldwide. the initial infection point is often a single compromised identity, whether that be human or non-human. Leveraging Zero Trust and least privilege principles, the CyberArk platform monitors and manages how sensitive data and assets are accessed to better secure all user types across hybrid and cloud environments, business applications, and throughout the DevOps lifecycle."

#### TENABLE AGREES TO ACQUIRE CYMPTOM

Tenable Holdings, Inc. the cyber exposure company, has signed an agreement to acquire Cymptom, a leader in attack path management.

Headline breaches, be they advanced persistent threats, ransomware or common hacks, routinely exploit well known attack paths in enterprise networks. Identifying, understanding and disrupting these attack paths before attackers can exploit them is critical to reducing the probability of a breach. Cymptom enables organisations to continuously test and evaluate threats according to the MITRE ATT&CK framework and the hacker's attack perspective, without the use of agents or running simulated attacks. Combining Tenable's marketleading coverage of vulnerabilities and misconfigurations with Cymptom's unique attack path analysis and prioritisation

NICO POPP

capabilities will enable security teams to pre-emptively

focus response ahead of and during attacks.



## SANS INSTITUTE ANNOUNCES INTERACTIVE TRAINING PROGRAM FOR NEW GENERATION OF CYBERSECURITY LEADERS IN SAUDI ARABIA

#### SANS Institute, the global leader in

cybersecurity training and certifications, has announced the SANS Secure Middle East 2022 training program, which will be held in-person at the Crowne Plaza Riyadh RDC Hotel & Convention Centre, from March 19 to 31, 2022. At SANS Secure Middle East 2022, participants will develop and master essential information security skills and techniques needed to secure critical information and technology assets, whether on-premise or in the cloud.

"The Kingdom of Saudi Arabia (KSA) ranks second to the US as a global leader in cybersecurity, yet due to the increase in digitalisation and an accelerated digital transformation spurred by the pandemic, we can see that the cyberattack landscape in Saudi continues to grow," said Ned Baltagi, Managing Director, Middle East and Africa at SANS Institute. The GCC region has been a hotspot for cyberattacks since the start of the pandemic, with the Middle East facing an

NED BALTAGI

unprecedented wave of cybersecurity threats. In Saudi

Arabia, according to a recent VMWare report, a survey of 252 Saudis indicated 84% stated cyberattacks had increased due to remote working conditions, reinforcing the need for more accessible security information and upskilling practices.

"At SANS we encourage students to develop dynamic and proactive security strategies built on a foundation of detection, response and prevention," Baltagi added. "Events such as SANS Secure Middle East 2022 provide an opportunity for professionals to enhance their approach and revitalise their confidence in managing and leading security teams, ultimately becoming all-rounder experts in cybersecurity," he pointed out.

### GATEWATCHER SIGNS STRATEGIC PARTNERSHIP WITH ALJAMMAZ TECHNOLOGIES

**Cyber-attack detection solutions** provider Gatewatcher and leading Saudi distributor Al Jammaz Technologies have signed a strategic partnership to enable the deployment of Gatewatcher's AlonIQ detection and response platform (NDR) marketing strategy in The Kingdom of Saudi Arabia and GCC region.

Gatewatcher, the European leader in intrusion and advanced threat detection, offers a range of solutions that provide an immediate improvement to current cybersecurity issues and a response adapted to the new detection needs of organisations thanks to a 360° view of cyber threats. These solutions, developed using artificial intelligence, offer a flexible (cloud, on-premises, hybrid), scalable, innovative approach, open to new technologies, without disrupting the existing architecture. They also facilitate the operations

of cybersecurity teams for better efficiency in prioritising their remediation actions. According to the agreement, enterprise customers benefit from the joint expertise of both entities to confidently provide the highest level of protection, detection and response to cyber-attacks.

"We're excited about this partnership and look forward at empowering our channel partner ecosystem to assist customers in dealing with emerging cyberthreats and mitigating them. Cybersecurity is first and foremost about innovation for the defence of customers digital Infrastructure and cyber footprint. Our alliance with trusted partner like Gatewatchers in the detection of the most advanced threats is at the heart of addressing all of these issues," said Asim AlJammaz, President at AlJammaz Technologies.

#### ACRONIS LAUNCHES FIRST CLOUD DATA CENTER IN NIGERIA

#### Acronis, the global leader in cyber

protection has announced the availability of a new Acronis Cyber Cloud Data Center in Lagos, Nigeria. The new data center, one of the 111 new data centers being deployed by the company, gives service provider partners access to a full range of cyber protection solutions upon which they can build new services while delivering faster access, constant data availability, and data sovereignty to their clients.

Having these capabilities is key for Nigerian service providers today, as cyber threats loom over the business landscape and data accessibility, privacy and compliance demands grow.

The opening of the Nigerian data center is part of the Acronis Global/Local Initiative, an effort that includes global management for all data centers, geographic redundancy, and control for local partners, and a local disaster recovery site – all with competitive pricing. The goal of this initiative is to ensure service providers will have no trouble meeting the ever-changing compliance, data sovereignty, and performance requirements they and their clients face.

At an event that took place in the heart of the city, leaders from the industry and special guests all gathered to celebrate, such as Tony Ojobo, President of the Board of Trustee of the ICT Foundation and Former Public Affairs Director of the Nigerian Communications Commission (NCC).

From Europe to Asia and from the US to Africa, Acronis already opened cloud data centers across the globe and is planning to open many more. With the new data center in Nigeria, local service providers will have a location within the country where they can store business-critical data for their clients. Managed service providers (MSPs) will also benefit from the full range of managed cloud solutions and cyber protection solutions available via the Acronis Cyber Cloud platform.



## LEADING THE WAY



hady Youssef is one of the most decorated and distinguished IT leaders in the Middle East, and in a compelling interview he discusses the trends driving changes in the datacenter ecosystem, the exponential increase in connected devices – and how Leviton's products are ensuring they remain a market leader.

It has been well documented how the pandemic has accelerated and driven the demand for larger datacenters in the current digital economy we are immersed in.

Youssef highlighted how they have witnessed an increase in the adoption of online entertainment services at home and connected IoT devices, which has rather inevitably led to this exponential growth in data needs.

According to the Managing Director at Leviton, there has been a particularly rapid growth in the Middle East, but claimed Leviton are very well positioned and poised to cope with that growth.

"If we take a closer look at how things are changing then a perfect illustration of that is the fact there is 7.2 billion people on the planet, however, in 2020, there was 50 billion IoT devices connected to networks, now that's an incredible example of how connected our society has become. As individuals, we all have a smartphone, a tablet at home, and a wearable device and what all these devices have in common is a hunger for bandwidth and our solutions have got the ability to meet these bandwidth demands.

Youssef added that in relation to trends, they have seen the emergence of a lot of edge datacenters and that has been driven by 5G, IoT and online gaming in addition to Hyper Scale datacenters.

"In 2022, the estimated IP traffic is around 20+ zeta bytes, which really is

"WHAT IS IMPORTANT IN THE DATACENTER ECOSYSTEM TODAY IS NOT ONLY THE PRODUCT, BUT THE CAPACITY OF THE VENDOR TO UNDERSTAND ENDUSER NEED AND POSITION SCALABLE SOLUTIONS IS CRITICAL."

astronomical, and it is the reason why there is so much demand for more datacenters, not only in the Middle East, but across the world," said Youssef.

Driving innovation has been in the DNA of Leviton ever since its inception all the way back in 1906, and it continues to be an industry leader. A good example of that has been its leadership in the datacenter space with the evolution of its Category 8 Copper and industry first Single 24 Fiber MTP Connectivity Solutions.

"We were the first company in the industry to have an end-to-end RJ45 category 8 platform approved. Category 8 is specifically designed for datacenters delivering 25/40G Over Copper where the distances between switches and servers are short, and it is essentially an end-to-end solution for datacenters. We were also the first company in the world to have 24 fiber in a single connector, and what that means for our clients is it gives them the ability to migrate from 10G to 40G and 100G which maximises their return on investment," said Youssef.

Interestingly, Youssef said that a key component for success in the datacenter industry isn't limited only to the product, stressing that vendor capacity to support



scalable design and solutions.

"What is important in the datacenter ecosystem today is not the product only, of course the product is important, but the capacity of the vendor to bring scalable solutions is critical. Leviton's capacity is not just products, we are a huge manufacturer, and we have in-house expertise to understand the customer needs and we are able to tailor the right solution specific for them," said Youssef.

Youssef outlined the impact of its e2XHD solution and said that its ability to give customers flexibility was a gamechanger.

"The e2XHD is a hybrid datacenter platform for fast deployment, so it is like a plug and play solution where everything comes from the factory, and it gives you the possibility to put both fiber and copper on the same chassis. It reduces space and the more you can put in the datacenter enables you to get more clients in terms of co-location, which in turn generates more revenue for your company. Flexibility is so important as scalability that it provides for end-users," said Youssef.

The Managing Director of Leviton
Middle East then turned his attentions

to their Zone Cabling and white patch panel technologies.

"We launched Zone Cabling technology in 2003, but what was missing is the adoption. Zone cables have been designed specifically for the challenges in the data center environment by being smaller and lighter than equivalent conventional cables. Zone cables support 10 Gigabit Ethernet (up to 65 meter permanent link), Power over Ethernet, voice, and broadband video transmissions

"AT LEVITON, WE
EVALUATE SUCCESS
BOTH INTERNALLY
AND EXTERNALLY, BUT
WHEN YOU SEE THAT
YOUR COMPANY IS WELL
POSITIONED TO GROW AND
YOUR TEAM IS ENERGISED
AND GOING THE EXTRA MILE
TO ENSURE SUCCESS, THEN
THAT IS A KEY METRIC OF
SUCCESS TO US."

at frequencies up to 500MHz.As we continue to share our expertise and application driven solutions, we have recently seen an increased demand for zone cables. With everyone aligning to Sustainability and Green Initiatives, white panels are gaining traction in the datacenter and that is part of Leviton product portfolio," said Youssef.

In terms of its success during the pandemic, Youssef credits a motivated and driven team as a key element in its continued market success across the Middle East.

"At Leviton, we evaluate success both internally and externally, but when you see that your company is well positioned to grow, and your team is energised and going the extra mile to ensure success then that is a key metric of success to us. We really succeeded during the pandemic in terms of delivering major critical infrastructure projects in industry verticals such as healthcare and banking, achieved amidst the backdrop of a volatile and unpredictable climate caused by the COVID19 pandemic. This was a huge achievement for us, and we are looking forward to 2022 with great hope and optimism," said Youssef. 1



Unlock the performance of your computer with Crucial P2 NVMe SSD



Capacities 250GB, 500GB, 1TB, 2TB Impressive speeds up to 2400MB/s4



#### Do More. Wait Less

Experience the NVMe™ difference. The Crucial P2 unlocks the performance of your computer, delivering shorter load times and faster data transfers¹.

Capacities	Sequential Read	Sequential Write
2TB	2400MB/s	1900MB/s
1TB	2400MB/s	1800MB/s
500GB	2300MB/s	940MB/s
250GB	2100MB/s	1150MB/s

#### MAXIMIZE YOUR INVESTMENT 5 - YEAR LIMITED WARRENTY





# BUILDING DIGITAL TRUST

GBM IS THE LEADER END-TO-END SOLUTION PROVIDER, OFFERING THE REGION'S BROADEST DIGITAL SOLUTIONS PORTFOLIO, INCLUDING DIGITAL INFRASTRUCTURE, DIGITAL BUSINESS SOLUTIONS, SECURITY AND SERVICES. IN A DETAILED INTERVIEW WITH ANITA JOSEPH, **HANI NOFAL,** VICE PRESIDENT OF GBM DIGITAL INFRASTRUCTURE SOLUTIONS DISCUSSES THE NEED FOR DIGITAL TRUST TO UNDERPIN THE SECURITY ARCHITECTURE OF ORGANISATIONS. A SECURITY ADVISOR EXCLUSIVE.

#### n the context of today's accelerated digital transformation, would you agree that security is the biggest challenge?

Yes, I'd say it is. Digital transformation does indeed bring in many security challenges, since data is growing y, in both value and volur

exponentially, in both value and volume. In fact, data is the cornerstone of digital transformation, driving businesses to tap into its potential and use its power to compete in the changing marketplace. However, this process of digital transformation exposes data to greater security risks, and cyber criminals are keen to exploit its value through theft, fraud, ransomware and other kinds of cyber-attacks.

This is what gets organisations trapped in a "digital deadlock," which keeps them from successfully transforming. So, organisations need to embrace opportunities for digital transformation, while keeping themselves, their data and their customers protected. How do they do it? The answer is, naturally, through effective cybersecurity.

However, designing and implementing a security strategy and architecture to meet the needs of data-driven organisations is easier said than done. Organisations in the region need to be fully equipped to meet the security challenges brought about by digital transformation.

### It's not just enough to transform, it's important to transform securely-how is GBM helping companies in their digital transformation journey?

With the acceleration of digital transformation, organisations are leveraging technology to redesign customer and employee engagement, transform operations and adopt new business models to address rapidly changing industry dynamics and user needs. As organisations reshape

themselves to adapt to the expanding digital economy, building resilience and trust into the digital experiences of customers, employees and partners is becoming increasingly critical.

There is a realisation now that security needs to be central to the digital architecture of the future enterprise to engender trust and resilience.

However, developing a digital strategy where security is "baked in" and not "bolted on" is challenging, and requires an understanding of risks across all facets of the enterprise and attention to building comprehensive security strategies to address them. At GBM, we help organisations build these security strategies.

In our annual security report last year, we found out that the top 5 focus areas for security initiatives were data security, secure remote access & connectivity, cloud security, identity & access management and endpoint device management. We have the capabilities and expertise to develop an



themselves and create greater confidence in security, safety, privacy and reliability among consumers.

Digital trust is built up over time based upon our actions, processes and, in the case of businesses, our ability to fully address the business risks that cyber threats bring with them. Organisations need to include cybersecurity at the heart of the digital trust. This helps to ensure that the organisation is not avoiding security measures just to get their service or device on the market. By aligning the cyber security investments to the desired business outcome of trustenabled commerce, we can more clearly understand the importance and value of our cybersecurity investments even if we have not experienced a hack.

It's also important to highlight that the tools we invest in for security need to evolve from perimeter security, to one of distributed integrity, one component of which is the currently popular Zero Trust model – where we have a better understanding of high and low risk areas and can adjust our monitoring focus. Adopting the zero-trust model decreases the number of opportunities a hacker accesses secure content by limiting who has privileged access to different machines or segments of the network.

GBM's Security Report 2022 which will be launched soon, dives deep into how security should be central to discussions on digital trust.

#### How does digital trust impact the wider society?

Digital Trust is the conversation that we need to be having across all levels of society, which includes individuals, businesses and governments.

There is a growing need to monitor critical assets and systems, better sense when unexpected activities take place and take the right type of

ORGANISATIONS IN THE REGION NEED TO BE FULLY EQUIPPED TO MEET THE SECURITY CHALLENGES BROUGHT ABOUT BY DIGITAL TRANSFORMATION.

action to respond to a full-scale breach before it can manifest itself. Achieving this trust requires a "partnership" between individuals, businesses and governments. In this cyberwar, the partners as a group are on one side, while the threat actors are on the other. We need to align the expectations of each partner and look carefully at what each of them require:

- Individuals have the desire to have instant online secure access to their favourite products and services
- Governments have the desire to protect their populations and commerce
- Businesses have the desire to profitably serve customers

Now, all three groups have roles to play in the goal of engendering mutual online trust that benefits all of society, whilst reducing the opportunities for threat actors to negatively impact any of us.

Let's begin at the individual level. The pandemic forced many people to work remotely and many people used telemedicine for the first time. Similarly, the use of video conferencing apps skyrocketed. These changes brought many security risks that most people weren't aware of. So, now, individuals should -more than ever- be careful about what they share online, especially employees have an extra fiduciary responsibility to ensure they do not become the threat vector for their employers. According to the GBM Security Report 2020, 66% of

organisations found that managing identities and access of end users were a challenge, especially in multi-hybrid cloud environments.

For business users, the implication of a breach is more significant. Aside from the data concerns, there are significant operational and even potential lifethreatening concerns to take into consideration. Recent research suggests that that one third of all organisations in the Gulf are experiencing revenue slowdown, in which case the costs associated with a breach could have a more negative impact. That's why the digital trust concept is now more crucial than ever because organisations cannot afford to lose customer trust or fall victim to a breach.

Now let's move to governments. They play an important role as facilitators



of how data is governed to protect the rights of businesses and individuals, while driving economic growth and social good. The digital-first mindset of businesses and governments in the Gulf has also increased awareness about the way data is collected, processed, stored, shared and maintained. Over the last decade, there have been a number of new laws passed in the region to regulate data governance, like the DIFC Data Protection Law in the UAE and the Personal Data protection Law in the Kingdom of Bahrain.

#### What will 2022 bring to the Gulf region in terms of cybersecurity challenges?

Organisations are now seriously considering how they will respond to a cyber-attack or breach, whilst maintaining the trust of their community.

TRUST IS THE
CONVERSATION
THAT WE NEED
TO BE HAVING
ACROSS ALL
LEVELS OF
SOCIETY, WHICH
INCLUDES
INDIVIDUALS,
BUSINESSES AND
GOVERNMENTS.

They have reprioritised risks post the pandemic. In our security report we identified 8 kev risks that radically shifted in priority for Gulf organisations. The top risks include growing end-user security risks, risk of cloud security breaches, growing identity risks, risk of data and service availability in distributed environments, risk of internal delays to incident response and data and privacy risks due to unsecured applications. These concerns are the main drivers of security investment focus areas which we uncovered in our report. Organisations are now planning to focus on data security, secure remote access, cloud security, identity & access management and endpoint device management on their investment plans, which are clear reflections of the risks reprioritised.

Data security tops the list of concerns, and for a very good reason. Traditionally, data management has been the role of the storage team, however this group have never been formally tasked with responsibility for the security of data. Likewise, the cybersecurity team has traditionally been responsible for securing systems, network and applications. We are at a pivotal point in data management and cyber security where organisations must decide where this responsibility lies. Mature data management is a complicated issue; hot, warm and cold data of varying degrees of business and compliance importance exist both on and off-premise.

For cybersecurity professionals, the move to cloud has revealed the need to consider data security, as well as some new legislations, but until recently this was never a focal point. This needs to change.

Concerns about remote access are well-justified. With many working from home or in a hybrid model, the network perimeter has evaporated and IT teams in many markets are having to manage the security of home networks to secure their own corporate ones.



# ACHIEVING THIS TRUST REQUIRES A "PARTNERSHIP" BETWEEN INDIVIDUALS, BUSINESSES AND GOVERNMENTS.

For many the focus on endpoint as well as identity and access management could address not only the remote working concerns, but also cloud access and data security issues.

Ensuring only the legitimate users and devices are access data, with integrity, can help to resolve many of the risks faced by security and data management professionals.

#### What about the cybersecurity skills gap? Is it a concern for organisations in the Gulf too?

Absolutely. Finding the skills to address cybersecurity has always been a key challenge. GBM's Annual Security
Report 2020 mentioned that 64% of organisations in the region currently face challenges in addressing skill gaps. In the early days of IT security, the demands were very network-centric, with firewalls, VPN, and network monitoring occupying centrestage.
Today, however, this is a highly datadriven discipline and the need to have strong data analytic and interpersonal interrogative capabilities are higher.

With many organisations observing millions of potential threat alerts daily, the ability to program the tools to identify the "signal" of a possibly

malicious event from the "noise" created by networks and underlying protocols is becoming the key differentiator of a successful cyber defender.

Organisations in the GCC should transcend this by implementing a more proactive monitoring and response mechanism to mitigate potential security risks and including a Security Operations Centre (SOC) and a Security Incident and Event Management (SIEM) platform to tackle these challenges. More importantly, having a skilled and experienced IT security team is important to implement and operate such platforms successfully.

Therefore, there is heightened advocacy for working with Managed Security Service Partners-organisations who make cybersecurity their business, as such organisations can invest more into cybersecurity since it is their business. Clearly, the risk is not outsourced, but there are many tasks within the cybersecurity arena that should be outsourced. Managed Security Services are becoming a priority across Gulf.

#### What advice would you give organisations to ensure digital trust in security?

The explosion of online economic activity that began in 2020 is not slowing down. At the same time, cyber-attacks will not be slowing down, either.

There are two sides to this ongoing cyberwar: cyber criminals vs the

targets. Cyber criminals are a well-funded, highly motivated set of conglomerates and cooperatives that share intelligence, tools, processes and best practices. They use cryptocurrency to successfully get paid, but hide their identities, have cybercrime-as-a-service offerings and are generally, extremely financially successful. The pandemic brought to this group a fresh set of new opportunities to make more money.

The targets unfortunately do not work together to overcome the enemy and act as individuals in this war. Their governments do what they can to protect them and their customers, but ultimately extract fines when the targets get hacked.

There are certain steps that should be taken to improve this situation:

- 1. Government regulators should mandate the sharing of breach data since we learn more from others mistakes then their best practices. Fines and regulation should focus on breach disclosure and adequate security controls being in place
- 2. Enterprises must realise they are fighting a war against experts and need expertise to help it cannot be won alone.
- 3. Technology and service providers need to work with both groups as technical advisors, to help identify how best to implement and apply regulations, and how best to comply with said regulations.

Achieving these goals will be a journey, but if enterprises and

governments don't all agree on the direction we are to be heading, we will not be able to succeed.

As we can all imagine, cybercrime may never be eradicated, but we should be able to reduce the impact and burden to enterprises and individuals if we work together more effectively.

Zooming into the enterprise perspective, enterprise trust needs to embrace customers, employees and business partners.

The customer relationship is often more keenly focused upon, and clearly adhering to customer expectation towards data privacy and online security is more critical than simply complying with legislation – customers expect more than this.

Employees, who are the front line in any customer engagement, need to feel safe and secure in their working environments, which must translate into secure devices, identities, systems, and a simple way to ensure this remains so. Arduous security processes will create friction at an employee level which can leak into customer interactions.

Business partners are becoming more digitally connected and so ensuring an enterprise's integrity within the industry supply chain is becoming a requirement these days.

All areas demand a robust risk management capability: understanding the risks to the enterprise and its connected ecosystem, understanding that not all risks are the same and applying the appropriate level of control for the identified risk.

Cybersecurity is rapidly evolving into a highly targeted, risk-based, practice that is also agile enough to respond to the changes in risk profile of an enterprise. Only by doing so can an organisation become capable of improving its scores in the cyberwarfare we are all engaged in today.

FOR CYBERSECURITY PROFESSIONALS, THE MOVE TO CLOUD HAS REVEALED THE NEED TO CONSIDER DATA SECURITY, AS WELL AS SOME NEW LEGISLATIONS, BUT UNTIL RECENTLY THIS WAS NEVER A FOCAL POINT.

# IDENTITY PROTECTION TO BE A PRIORITY IN 2022

RAY KAFITY, VP – MIDDLE EAST TURKEY AND AFRICA (META) AT ATTIVO NETWORKS



very year, IT and cybersecurity firms round up their predictions on their expectations for the immediate future. While predictions have a particular pull factor in the marketing sense of the word, we at Attivo Networks share our evidence-based forecasts into cyberattacker behaviour and tactics, techniques, and procedures (TTPs).

The 2021 Verizon Data Breach report highlighted that 61 percent of breaches involved credential data. If there is one thing we can learn from 2021, it is that cyber attackers focus on credentials to expand their reach into their victim's networks, such as the Colonial Pipeline incident (where fuel shortages resulted from a single compromised password).

In the coming year, the focus for defenders should be on technology and solutions that can detect and derail such attacks before they can cause great harm to the organisation.

#### Enterprises will increase their investment in identity security solutions.

The rise in third-party attacks, remote working security risks, and the continuing evolution of ransomware have driven

home the fact that traditional security solutions are no longer enough. And while existing solutions like Identity and Access Management (IAM), Privileged Access Management (PAM), and Identity Governance and Administration (IGA) provide basic identity protections, their focus on authorisation and authentication leave gaps for attackers to exploit. To close those gaps, enterprises need to invest in Identity Detection and Response (IDR) solutions capable of providing expanded exposure visibility and detection specific to credential misuse, excess entitlements. privilege escalation, and other common identity-based attack activities.

#### Ransomware defences must get a badly needed refresh.

Ransomware 3.0 is here, characterised by double extortion, where cybercriminals encrypt files and leak information online to drastically impact the company's image, profits, stock price, and more. There's no longer a one-size-fits-all approach to defending against these attacks. With over 300 variants, stopping ransomware requires a multi-faceted approach that starts with protecting Active Directory and privileged credentials. In 2022, organisations won't understand how each group operates and, instead, must improve their visibility to exposures and add detection measures based on techniques. Setting up traps, misdirections, and speed bump lures along the way will also serve as strong deterrents to keep an attacker from succeeding.

#### Active Directory (AD) protection, a top CISO-level concern

AD is an essential element of an enterprise's network infrastructure, but it is intrinsically insecure and notoriously difficult to protect. Attackers are aware of its weaknesses and diligently target AD to increase their privileges, escalate their attacks, and mass-encrypt data for ransom. Mandiant, a leader in incident

response services, named Active Directory exposures the top reason ransomware attacks continue to be successful.

Business leaders and IT decision-makers cannot afford to let visibility and organisational divides leave exposures unaddressed and open for attack.

#### Insurance companies will raise rates and technology requirements.

Cybersecurity Ventures estimates that ransomware costs will reach \$265 Billion by 2031, with an expected 30% year-over-year growth in damage costs over the next ten years. To help minimise their risk, insurance companies will increase their premiums and institute stringent security technology requirements as a prerequisite to extending coverage or making payouts. With Active Directory being a primary factor in almost every ransomware attack, insurance companies will look favourably at systems that detect innetwork lateral movement and credential misuse, seek privilege escalation, and

THE RISE IN
THIRD-PARTY
ATTACKS, REMOTE
WORKING SECURITY
RISKS, AND THE
CONTINUING
EVOLUTION OF
RANSOMWARE
HAVE DRIVEN
HOME THE FACT
THAT TRADITIONAL
SECURITY
SOLUTIONS ARE NO
LONGER ENOUGH.

protect identity management systems, such as AD.

#### Supply Chain issue to increase complexity and risk

Supply chain issues force enterprises to order supplies months in advance, in larger quantities, and from new providers. The lack of supply will add complexity to new vendor management and qualifications as organisations adjust their purchases, and potentially standards, to support business operations. This change will introduce new supply chain security risks that could arise from software, hardware, and logistics security exposures.

#### Skill gap to impact attraction and retention policies

Women and single parents were disproportionately impacted by the pandemic when it came to their careers. With many employees stepping away from their jobs in 2021, combined with the skilled IT shortage and the anticipated Great Resignation of 2022, organisations will continue to compete to attract and retain highly skilled cybersecurity talent. Companies that offer robust benefits and perks, remote working, flexible hours, and subsidised childcare will come out on top in the battle for talent.

As we head into 2022, one thing for certain is that it is not a matter of whether attackers will breach Middle East organisations but when. With the over-emphasis of sophisticated attackers to compromise identities, CISOs need to include Active Directory in their cyber hygiene and posture management programs and look for continuous visibility capabilities when selecting technology to prevent and detect AD vulnerabilities, threats, and attacks. These capabilities include high visibility for AD vulnerabilities and exposures, detecting live attacks, and discovering misconfigurations.





ata Management is, arguably, the biggest challenge facing business today as they accelerate their digital transformation goals and fast-track their arowth momentum. This inevitably brings the guestion of data protection and security to the fore, as

breaches and attacks become more complicated, sophisticated, unpredictable and serious. Data Privacy Day, observed every year on January 28, serves as a reminder to us to assess how our data is being used. It provides the perfect opportunity for companies to take stock of their security practices and understand the whole data ecosystem.

> "AS MORE OF OUR **LIVES ARE DIGITISED AND DATA VOLUME CONTINUES TO GROW, CITIZENS AND BUSINESSES FACE AN UPHILL BATTLE** TO PROTECT THEIR **DATA & PREVENT** THREAT ACTORS FROM USING IT IN THE SERVICE OF CYBERCRIME AND FRAUD."

#### So, what is data privacy and why is it important?

With data becoming more voluminous and its users more dispersed, awareness about how information is being used, collected or shared is also scattered, with no proper security checks in place. Data Privacy Day signifies a global effort to reinforce the need to channelise critical data management practices and create culture of zero-tolerance to careless cyber hygiene and practices. Today, however, data privacy has become more than just an effort-it's a crying need.

According to Brian Pinnock, Cybersecurity Specialist at Mimecast: "As more of our lives are digitised and the volume of personal and corporate data continues to grow, citizens and businesses face an uphill battle to protect their data and prevent threat actors from using it in the service of cybercrime and fraud. Personal data has become like gold to cybercriminals, who weaponise your own information against you to make their cyber scams more believable."

"It is imperative that Data Protection solutions adopted by companies are reviewed regularly to ensure they have a well-tested and proven data recovery plan in place," says Charles Smith, Consulting Solution Engineer – Data Protection, EMEA at Barracuda.

In other words, it's vital to understand rather than just pay lip service to the regulatory language of the day or stand by and watch our privacy erode as we downplay its importance and become more and more desensitised by the minutiae of the latest breach.

Put it simply, data privacy should be taken more seriously than it is right now, particularly in today's day and age, when the cyber threat and security landscape is highly volatile and complicated. But





**Bernard Montel,** EMEA Technical Director and Security Strategist at Tenable



# "IT ORGANISATIONS CONSTANTLY MANAGE LARGE AMOUNTS OF DATA THAT REALLY DOESN'T MATTER ANY LONGER."

then, as Joseph Carson, Chief Security Scientist & Advisory CISO at Delinea puts it: "The notion of real 'privacy' is perhaps something that no longer truly exists. Internet connected device usage has exploded in recent years, bringing huge changes to our society, but this has come with risks as we're all tracked and monitored 24/7."

This, however, means we need to act, and fast.

"It means we need to consider not just data privacy, but the safeguards that govern how data is collected and processed. Thanks to stricter regulations, the public now has greater say on how their data is used, but regulatory bodies need to continue to pressurise companies and governments to maintain good cyber security practice, incorporating the principle of least privilege to protect collected data and

provide users with transparent access to such data," Carson adds.

#### THE DATA LANDSCAPE

Unfortunately, data privacy remained shrouded in mystery and misunderstandings for a very long time. Because many companies viewed data privacy purely as an IT issue, they only had it incorporated into their larger disaster recovery plans.

Rick Vanover, Sr. Director of Product Strategy at Veeam comes straight to the point when he says that should no longer be the case. "Privacy matters. Data Privacy continues to be more important than ever. From an awareness standpoint, Data Privacy doesn't get the attention it needs. I see IT organisations constantly manage large amounts of data that really doesn't matter any longer. ROT - Redundant, Obsolete or Trivial - Data should be moved out of its storage lifecycle. My practical advice on Data Privacy day is to assess what data is where and identify what needs to be removed. If it doesn't need to be removed. then determine if selected data should be moved to a correct tier or policy. From a privacy perspective, where it exists is an important first step of the process."

Today companies are waking up to the reality that cannot afford to skirt the issue any longer.

"If the last few years have taught us something, it is the fact that digital security has an impact on both consumers and businesses, says Saket Modi, Co-founder & CEO at Safe Security. "Whether it is the leaked credentials of customers on the Twitch hack or the leak of Pandora papers, data protection and cybersecurity are on top of everyone's agenda. There was a surge of cyberattacks than ever before throughout 2021, and according to data from Check Point Research corporate networks saw 50 percent more attacks per week



**Charles Smith,** Consulting Solution Engineer – Data Protection, EMEA at Barracuda







**Joseph Carson,** Chief Security Scientist & Advisory CISO at Delinea

when compared to the previous year, and yet businesses continue to depend on traditional methods of cyber risk management." Brian Pinnock concurs.

"The rapid digital transformation that most businesses have had to undergo in order to adapt to pandemic-related challenges and a new hybrid working world, has created additional opportunities for threat actors, who have stepped up their efforts to breach organisational defences and steal sensitive personal and professional data," he observes.

"COMPANIES MUST
WORK WITH THEIR
IT TEAMS TO BUILD
VISIBILITY INTO
THEIR DATA AND
WHO HAS ACCESS
TO IT, AS THIS WILL
ENABLE THEM
TO MAKE BETTER
SECURITY DECISIONS
THAT ENHANCE DATA
PRIVACY."

Changing customer attitudes have also added to the increased focus on data privacy, says Saeed Ahmad, Managing Director, Middle East and North Africa at Callsign.

"Over the past few years, consumer attitudes and expectations around data privacy and security have shifted, influenced by the increased publicity about data breaches, Apple's move to enable opting out of app tracking, Google's move to block third party cookies and our increased life online."

Gregg Ostrowski, Executive CTO at Cisco AppDynamics holds the view that in this post-pandemic era, a strong security posture means organisations have the necessary processes in place to protect their applications and their business from vulnerabilities and threats. "In a world where sensitive data is constantly at risk of being compromised by malicious actors, they must be prepared and strengthen their security posture, enabling them to predict, prevent and respond to threats," he adds.

However, despite all the increased attention, it was popularly 'misunderstood' that data privacy centred around sensitive data within files and databases. "The written word is not the only concern," points out Morey Haber, Chief Security Officer at BeyondTrust. "Audio, video, and biometrics are also

Morey Haber, Chief Security
Officer at BeyondTrust

governed by data privacy regulations and should have appropriate controls to identify content and protect them accordingly. As an example, this includes cameras in home and offices and audio recordings from a call center that may be used for training purposes."

#### THE APPROACH

As vast an area as data privacy is, it needs to be seen in perspective. Perhaps, the best way to think about the privacy issues is to imagine the world using Tinkertoy as an analogy, says Sam Curry, Chief Security Officer at Cybereason. "Tinkertoy sets are used

to build structures made up of hubs and connecting rods. This is analogous to us all with the hubs or "nodes" being people, objects, computers and data and the rods or "edges" being the relationship among us like "child of," "owned by" or "used by." This massive structure could be taken to a ridiculous extreme and could. theoretically, represent the entire world in a shifting, powerful construct. We have a branch of mathematics ideal to this sort of mapping called Graph Theory; and this is exactly what data aggregators like Google, LinkedIn and Facebook do — they mine the metadata about the structure and sell it for money."

Understanding data privacy also means taking the time to learn what privacy controls are available in all the apps and online services that companies and their employees use. "Unfortunately, every app and every social network seems to do things differently, with privacy and security options often scattered liberally across numerous "settings" pages," points out Paul Ducklin, Principal Security Researcher at Sophos. "But don't be afraid to dig through all the options, and don't just rely on the default settings. Start by turning off as many data sharing options off as you can, and only turn them back on if you decide you really want and need them. If a service demands you to share more than you are willing to hand over - your address, phone number or birthday, for example - or asks for data that you just don't think is relevant for what you are getting in return, ask yourself, "Do I really







**Rajesh Ganesan,** Vice President, Middle East & Africa at Manage Engine



need to sign up for this, or should I find somewhere else that isn't so nosy?"

#### 2022-A Turning Point?

It's clear by now that much like 2021, data privacy will continue to hold considerable sway among businesses that seek to grow and accelerate their digital transformation journey, this year as well.

# 1.24 / AFFEE 19:10 / F

In the words of Gal Ekstein, General Manager EMEA & LATAM at AppsFlyer: "In 2022, we'll see marketers continue to adapt to the move away from user-level data towards aggregated data. In addition, predictive measurement will also play a greater role, both of which will be crucial in gaining meaningful marketing insights in a privacy-complicit way. Ultimately, marketers that are able to balance privacy considerations with a positive user experience will win out in 2022."

In order for data privacy to be effectively implemented, visibility must

"START BY TURNING OFF AS MANY DATA SHARING OPTIONS OFF AS YOU CAN, AND ONLY TURN THEM BACK ON IF YOU DECIDE YOU REALLY WANT AND NEED THEM."

become top priority for organisations, says Nicolai Solling, Chief Technology Officer at Help AG.

"Companies must work with their IT teams to build visibility into their data and who has access to it, as this is a critical step that will enable them to make better security decisions that will enhance data privacy, and subsequently improve regulatory compliance. This should then be followed by the implementation of a Zero Trust data security model and privileged access management," he affirms.

Rajesh Ganesan, Vice-President, Middle East & Africa at Manage Engine is of the opinion that educating employees must take centrestage.

"Data protection is only successful when all components within the infrastructure—including all employees—are prepared to handle it. To do this efficiently, data protection must be built right from the design stages of all services and operations. Moreover, data protection should be present as a strong, invisible layer; it shouldn't hamper operations, nor should it require big changes or specialised training. It is best to educate people on the dos and don'ts of data protection in a way that is contextually integrated into their work, as opposed to relying solely on periodic trainings."

Aaron Louks, Security operations
Engineer at ThreatQuotient says that
a security tool is only as good as the
intelligence sources backing it. "Staying
up-to-date with the current threat
landscape through multiple intelligence
feeds is paramount for identifying
intrusion events and providing data
protection for your organisation. I'd like to
emphasise that it's advisable to diversify
your intelligence data because no single
feed is going to have a complete picture
of the threat landscape. It's important to





**Saeed Ahmad,** Managing Director, Middle East and North Africa at Callsign

have a layered approach so the probability of identifying and blocking malicious activity is improved," he adds.

Bernard Montel, EMEA Technical Director and Security Strategist at Tenable says companies must take a risk-based approach and gain a clear view of where their system vulnerabilities lie. "This includes understanding the entire scope of an attack path - how could an attacker get in, what could they do, where could they go and what are the implications of this incursion."

Sandra El Hattab, Cybersecurity
Consultant at Axon Technologies agrees.
She sums it up best when she says: "By
understanding its business context, an
organisation should identify the data
types it handles, assess the regulatory
environment it operates in, establish a
data privacy policy that matches business
practices and complies with laws and
regulations, create a suitable data
classification scheme, and implement
data handling controls and procedures.
The approach should also take into
consideration how data flows to third
parties and other external touchpoints."

"A great aspect of data privacy revolves around people. Investing in awareness programs that educate employees is crucial. Ultimately, security is as strong as its weakest link," she points out.



Officer at Cybereason

Sandra El Hattab, Cybersecurity

Consultant at Axon Technologies

# SECURITY. NO COMPROMISE.

**ALOYSIUS CHEANG,** CHIEF SECURITY OFFICER AT HUAWEI UAE, TELLS ANITA JOSEPH HOW THE COMPANY HAS ADOPTED A SECURE-BY-DESIGN PHILOSOPHY THAT INCORPORATES CUTTING-EDGE SECURITY INTO ALL ITS PRODUCTS.

ell us about the cybersecurity landscape in 2022-what are the trends we must be aware of?

Ransomware will continue its onslaught in 2022. So, this will be a key issue. And it's likely that ransomware will be evolved into targeting certain applications and OT/ IoT, and even autonomous vehicles could be hit. So that's one of the things we'll see developing and shifting gear this year. Additionally, Metaverse is something that cannot be ignored-either the convergence of the different worlds in the Metaverse will bring forth a new era, or everything will crash and burn with nothing left to spare. With the Metaverse becoming a reality in the near future, the boundaries of this universe are going to be very, very hard to define with a lot of grey areas with the entire ecosystem going to be more and more fragmented. So that's one of the reasons why regulators are always

trying to catch up, because it takes a lot of efforts to keep pace with all these new technology developments.

Therefore, I say that when all the dust settles, cyber security will be the key to deciding how we are going to address the adoption of Metaverse and what our strategy will be in supporting immediate digital transformation needs and our Metaverse future.

"CYBERSECURITY
WILL NEVER BE
SOMETHING WE
CAN COMPROMISE
ON. SO WE REMAIN
COMMITTED TO
ENSURE THAT IT'S
GIVEN THE TOPMOST
ATTENTION AND
ADDRESSED AT THE
HIGHEST LEVELS."

With remote and hybrid working becoming the trend now, the security of connected handheld devices is a huge concern. How is Huawei addressing this issue and what's your approach there?

I think our approach is very simple - promote a culture of cyber hygiene and build a culture of security within the companies, so that you will know how to maintain a cybersecurity green pass for not only our cloud but also all the endpoints. These days, every person will carry at least eight IoT devices with them. Personally, I have more than one mobile phone, and that means that I have more than one potential risk that I need to be aware of and address. So having a good cyber hygiene will help build a culture of security as the first key step.

Step two will be automation - relying on the power of the cloud to bring Al-powered security that will have you make the right decisions at the right time in the right place. Look at it this way: you have so many things to



end of the day, there is a maturity of security of endpoints today. 10 years ago, the security of the cloud was the talking point. Everybody was concerned about migrating to the cloud and risking losing all their applications, their control, and privacy. But today, the conversation is going the other way of the spectrum, which are the endpoints. Here again, the problem is magnified multi-folded, because when you look at the cloud, there's only a few providers like HUAWEI CLOUD and some others, but when you talk about endpoints, we are talking about billions and trillions.

#### Do you think 5G or any of the networks will add to the security concerns?

5G and cloud are the two fundamental pillars supporting digital transformation that we need to safeguard, in order for us to have a secure and resilient ecosystem as we move to the digital era. So obviously, we need to address the security of 5G and cloud, looking at them from different aspects.

The security landscape of 5G and the cloud is forever evolving. And that is why we shouldn't rest on our laurels. We thought that we know what cloud and cloud security are, and we've also heard a lot about the need to build security for 5G recently. Like for example, the GSMA together with 3GPP has issued the NESAS & SCAS certification for 5G equipment. So that's why last year at GISEC, we announced the formation of a 5G security working group with OIC-CERT and just a couple of weeks ago we have completed the development of the 5G security framework that is readymade for OIC member states within 8 quick months. The OIC 5G Security Framework is a living document that we will continue to maintain and update to address the evolving needs of the

5G & CLOUD ARE THE TWO FUNDAMENTAL PILLARS
SUPPORTING DIGITAL TRANSFORMATION THAT WE NEED TO SAFEGUARD, IN ORDER FOR US TO HAVE A SECURE AND RESILIENT ECOSYSTEM AS WE MOVE TO THE DIGITAL ERA."

new technology because whether is it 5G or cloud computing, these are new and emerging technologies that one cannot hope to solve the problem using traditional standardisation routes-because international standardisation are most effective when it comes to mature technologies given that any standard developed will stay relevant for the next 3 to 5 years minimally with very minor needs for any update. For emerging technologies such as 5G or cloud, we have to consider and expect that things will evolve every 18 months or even less.

So, to summarise, we need to look at 5G security as something new, every day. And for that reason, we have worked with OIC-CERT to develop the 5G security framework that was announced weeks ago to address the needs of OIC nation states especially in this region and that Framework will only get more relevant in time as we incorporate localised elements in the Framework as a living document

#### Have you planned any new security initiatives or strategies for 2022?

In Huawei, we have a long-term cyber security strategy, where we are still executing the strategy. In essence we have adopted a security- first mentality within the company, making cyber security the topmost priority within the company that permeates from person to process to department and business units, in the process implementing layered security or defence-in-depth, supported by a strong zero trust security model. As such. as we embrace the Metaverse, we have to ensure that all our products and services are secure by design. This means that we have to ensure that cyber security and privacy and protection mechanisms are inbuilt by design right from the beginning rather than as an afterthought.

We need to return to fundamentals by optimising and streamlining our processes. This includes looking at some of the issues and readdressing them based on our key strategy. Thus, we're going to make sure that when we look at any one of the new products or services that we're offering right now or any new products or services that will be offered in future, cyber security and privacy protection will be guaranteed out of the box to meet any compliance requirements or regulatory regime.

More importantly, from the perspective of the user, we will ensure that our users will have peace of mind when using our products and services, because their peace of mind is our peace of mind.

Cybersecurity will never be something that we can compromise on. So, we remain committed to ensure that it's given the topmost attention and addressed at the highest levels. Because in security, there is no compromise. This is our strategy for 2022.



# 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** 

CRN



ARN Innovation Awards

MITRE





tahawultech.com CISO50 & Future Security Awards 2021



# PUTTING THE CUSTOMER FIRST

KHWAJA SAIFUDDIN, SENIOR SALES DIRECTOR, MIDDLE EAST AT WESTERN DIGITAL, TELLS ANITA JOSEPH EDITOR, SECURITY MIDDLE EAST IN AN EXCLUSIVE INTERVIEW HOW THE COMPANY HAS THE CUSTOMER AT THE CENTRE OF IT ALL-RIGHT FROM PRODUCT DESIGN TO ITS EVENTUAL USE AND BENEFITS.

ell us about Western Digital's
growth as a company and the
science behind its products.
Western Digital as a company
was formed in April 1973 in
the US. We started by making controller
cards. AT that time, the only thing that
could help a human being compute was a

calculator. So that's how we started our journey in the IT-compute space. Slowly and steadily, we built up expertise in making storage devices.

Our storage devices are not centred around one specific application. That was our mantra-we're not going to offer just a 'vanilla' flavour and let the people decide. Instead, we sliced the needs of the end user into how he wants to use the application-whether it's in his mobile phone, laptop, PC, or in other ways where data is getting created. Then we identified the verticals and focused and designed the products as per the verticals. For example, around security

and surveillance, our Purple products are designed and manufactured for 24/7, 365-days uptime, because we know there are no downtimes in a camera vs a desktop product where you need everything but for a maximum use of around 8-9 hours vs cards which go into our mobiles, which is almost 24/7 usage. So, as a user, you want to click a button and capture that moment, because if you delay even by a few seconds, you lose that moment. These are the simple user experiences which we take back and then design a product.

So, for us, it's not just about selling a product-it's about creating an experience and making sure that the objective is met, for which people are putting their trust in Western Digital.

#### What were the products & solutions you showcased at the recently-concluded Intersec 2022?

At Intersec, Western Digital highlighted the importance of security and smart video needs with flexible infrastructure and data solutions to address applications from incamera recording to multi-stream AI and offer more choice. In addition, Western Digital also exhibited its WD Purple product range, engineered specifically for smart video and surveillance and includes three product solutions – WD Purple Pro HDD, WD Purple HDD and WD Purple microSD card. Offering improved efficiency for overall video playback, these devices bring reliable, surveillance-class storage that has been tested for compatibility in a wide range of smart video.

Moreover, the company also showcased its Ultrastar series of high capacity hard drives to support cloud service providers, telcos and system integrators. The Ultrastar DC HC560, with the first implementation of OptiNAND technology's capacity-enabling features, delivers an unbeaten 20TB1 capacity in a nine-disk platform (2.2TB/platter) with CMR recording format.

Here's the complete range of products we showcased at Intersec:

#### WD PURPLE WD Purple Pro (18TB)

Designed for advanced AI-enabled recorders, video analytics servers and deep learning solutions requiring additional capacity, performance and workload capability.

#### WD Purple microSD

Designed specifically for the mainstream security camera market. The card delivers a cost-effective combination of ultraendurance, high performance, and wide capacity range up to 1TB.

#### WESTERN DIGITAL ULTRASTAR Ultrastar DC HC560 20TB

The Ultrastar DC HC560 offers huge capacity to the market. It meets modern data center reliability requirements with 2.5M MTBF (projected) and a 5-year limited warranty. It offers security and encryption options to help protect data from unauthorised use, including SED models.

#### Ultrastar SN640

A mainstream NVMe SSD targeting broad deployment as boot, caching, or primary storage in data centre IT and cloud environments

#### Ultrastar Data60 JBOD Storage Platform

Designed for high density and flexibility, the hybrid storage platform is a key

FOR US, IT'S NOT
JUST ABOUT SELLING
A PRODUCT-IT'S
ABOUT CREATING
AN EXPERIENCE AND
MAKING SURE THAT THE
OBJECTIVE IS MET, FOR
WHICH PEOPLE ARE
PUTTING THEIR TRUST
IN WESTERN DIGITAL.

element of next-generation disaggregated storage and Software-Defined Storage (SDS) systems.

#### Ultrastar Data102 JBOD Storage Platform

The Ultrastar Data102 provides up to 2PB of raw storage in 4U using 20TB SMR HDDs in a compact and efficient form factor. The extremely dense form factor provides the flexibility to specify the HDD and SSD combinations for balancing capacity, performance, and cost.

#### What were the main learnings of 2021 and plans for the coming year?

If we look back at the times of physical distancing and social solidarity, as I'd say, what brought us all together was data. So we identified that data is one key bond which can keep us connected no matter where they are. Data isn't affected by travel curbs or restrictions of any sort-so that brought discussions on data consumption, sharing and accessing, whereby every house was transformed into an office, a classroom, or both, as the case may be. This created a huge uptake-not only in terms of demand, but also an understanding of the importance of data. It served to reiterate the fact that data is not something you can take for granted.

We also invested a lot in educating people about backing up data, identifying the right device for the right use, the various use cases, etc. So this was the major trend for 2020-21 and we have similar plans for 2022 as well. We will keep on enriching our end users about data as well as our offerings-not only our products, but also their features and benefits. The aim is to take away a 'capacity' or a 'price' discussion and focus instead on the features and benefits if our products and why they must be used. For instance, why an extreme card should be used for a digital camera vs an extreme pro for a drone, or why Purple should be used for surveillance, and so on. 1

# DATA-**POWERED** SECURITY

ANITA JOSEPH CAUGHT UP WITH JACK O'REILLY, DIRECTOR -**OEM & CCTV BUSINESS - MERAT** AT DELL TECHNOLOGIES, TO FIND OUT HOW THE COMPANY HARNESSES DATA FOR THE BEST OUTCOMES.



hat was 2021 like? There has been a big shift towards solutions that drive citizencentric outcomes which was further accelerated by the pandemic. So 2021 was really a year of acceleration. A lot of the solutions that have existed previously became more and more prominent.

These solutions are made possible by the amount of data that is becoming available. With so many more sources of data available like smart grids generating data, IoT generating data, autonomous vehicle data etc -we are seeing solutions like AI and ML becoming more and more popular. Dell Technologies can facilitate the harnessing of this data and use data analytics to generate the best outcomes and solutions. For instance, how do you turn data into the ability to live in a city with less traffic or less pollution in the air. And obviously, from a video safety point of view it is about making every citizen's life safer.

#### What are the main technology trends in the safety and security market today?

We're seeing lots and lots of different powerful technologies coming into play, like Artificial Intelligence, Machine Learning, 5G, etc. They're all bringing in brand new opportunities in the safety market and we're seeing that in 5G for instance, customers are looking at features like video surveillance on demand. Whereas before, latency may have been an issue, 5G is now solving that latency issue. So these are the technologies that sell, they're the big drivers that we've been seeing, and of course, this Edge concept where it's moving from the idea of things that are connected, to the actual data and how that is being addressed.

#### What are some of your new safety and security products & solutions today.

So, at Intersec 2022 held in Dubai recently, we were we were showcasing a couple

of different things. We were in the Tech Disruption zone, talking about our new validated design solution for airports, which is a specific framework that we have for building solutions for airport security.

What we do within this framework is we start by talking to our customers and understanding the outcomes that they're trying to deliver-obviously those outcomes require certain workflows, and those workflows require certain algorithms and functionality. What we then do is we look to our best-of-breed software partners that have the capabilities to support these workflows, and then assess them from both technical and business perspective. And then, once we add them, we begin our lab validation process. This is by far the most comprehensive lab validation in the industry.

We leverage our partnerships with Intel, with Nvidia, and we actually maintain mutual labs where these applications are brought in and tested on the various Dell platforms. Not only

are they tested for basic functionality, but our partners will also provide developer support to help them optimise their code on our platform. So we were launching this as an integrated solution at Intersec where we can bring our end customers in and our partners in to actually build their own solution with the help of our validation labs and our technology partnerships.

A good example of that actually is one analytics partner that could support seven streams per GPU card on a server. When they went into the lab, when they left the lab, they were able to do 70 streams per GPU on a service-obviously, dramatically reducing the cost per channel for our customers. This was something that we were talking a lot about at Intersec.

We've just launched our new gateway line as well, which is key for Dell at the Edge. Dell very much has an edge-to-core-to-cloud strategy, and our new gateway product was just launched a couple of weeks ago. That obviously, is fanless-it can work in rugged and dusty environments, and can be operated at temperatures of up to 60 degrees-so very relevant for this part of the world. And that's key for us when we're trying to drive the concept of analysing the data outside of the data center on the edge for more real time insights.

#### How do you think the growth of connected devices or IoT is impacting the surveillance industry?

I think that it's impacting us in one big way that we see, especially when we know there's two different types of security-the physical security and video surveillance, etc that we're talking about, and also securing the customers' network. And that's something that we're seeing within video surveillance and within all the different connected devicesit's more end points and access points back into the main network. And we definitely see this as one of the common challenges to the digital economy and the cybersecurity risks that are involved

with all these end points. We're seeing that around 80% of regional organisations have suffered a disruptive event in the last 12 months, which is 77% up from 2018, and so we're taking into account all aspects of protection, securing both above and below the OS and safeguarding that endpoint. And then there's additional options that ultimately protect the entire organisation. So that's the big thing that we've been seeing with the increase in devices-it's making sure that all of those devices are secure

#### What's the strategy for 2022 for the video surveillance sector in the region and what can we expect to see this year?

I think that within the OEM organisation, we've always had a very strong emphasis on technology partners. So a lot of what we do is we work with software companies that are looking to bring compliance to market or a bundled solution to market and that will remain a big a big part of our focus going into this year. This will be a big part of how we leverage those partnerships and how we work with our partners to put a turnkey solution either to the system integrators or directly to the end user.

WE'RE SEEING
THAT AROUND
80% OF REGIONAL
ORGANISATIONS
HAVE SUFFERED A
DISRUPTIVE EVENT IN
THE LAST 12 MONTHS,
WHICH IS 77% UP
FROM 2018, AND
SO WE'RE TAKING
INTO ACCOUNT
ALL ASPECTS OF
PROTECTION.

We've seen a lot of success in that market. But then also, if you look at the system integrators particularly in this region, it's around how we are giving them direct access to the Dell engineers, to the Dell video surveillance labs, so that they can also test and validate before any money is being spent, so that we can be absolutely sure that what those system integrators are bringing to their customers is validated and has gone through a live POC-so we re very much putting our focus on partnershipsthe ISV partners, the system integration partners and obviously the Dell channel partner program. We>re going to combine that with the strength of our CRS or cyber recovery solutions, because again, within this video surveillance market, cyber recovery is becoming such a big part. Also cybersecurity-we>re going to very much lean into that as well. Then, once again, the Edge is really becoming the new frontier, it's gaining pace with the rise of the IoT devices.

When you look at things like IOT and Al and machine learning-in the past. vou'd have video surveillance projects that were straightforward. You'd capture a video, you'd store the video and if there was an incident, it would either be caught by somebody sitting at a screen or it would be a case of going back and looking at old footage to see what had happened. But with the real time analytics that are coming now, with the need to have instant feedback on whatever it may be-traffic, left luggage, biometrics, temperature, thermal cameras-the immediate need to have those analytics is actually driving the size of the project. It's also driving the complexities of watching that the number of different technology partners that are involved in each project is growing. So, we're going to very much focus on that-how do we ensure that when we're working with our end customers, our partners, our OEMs that we are bringing that full suite of technology partners together to ensure that we get the best total solutions in the market. 1

## OREGON SYSTEMS, CYBERRES - A MICRO FOCUS LINE OF BUSINESS JOIN HANDS FOR DISTRIBUTION PARTNERSHIP

THE STRATEGIC AGREEMENT WILL BRING ENHANCED OT CAPABILITIES AND DIVERSITY TO THE SECURITY OFFERINGS IN THE REGION.

regon Systems, the leading
OT security distributor in
the Middle East region
and CyberRes-a Micro
Focus line of business,
have signed a strategic distribution
partnership for the Gulf region. This
collaboration combines the excellence
and expertise of both companies and
creates unparalleled opportunities for a
stronger and more diversified portfolio
of products and services in the region.

Commenting on the partnership, Manu Nair, General Manager, Oregon Systems, said:

"Being one of the frontrunners in ICS-cybersecurity in the region, Oregon Systems is committed to providing the right solutions to our channel partners and customers. We have been known to bring in new and specialised technologies to this region, especially in the OT/ICS Security domain. This collaboration will bring in greater value and add more depth to our product portfolio. The demand for OT SIEM is at peak and with Micro-Focus's current and future offerings, especially with the kind of references they have with regard to critical infrastructure clients, we're confident that we will be able to position the solution with multiple customers in the regions and fulfil the requirement."

With the collaboration agreement, Oregon Systems, with its extensive channel network and technical teams across the MEA region, will work closely with vendor expert teams to explore new opportunities and generate more brand awareness for Micro Focus.

Ibrahim Azab, Regional Sales Director, MEA, CyberRes – A Micro Focus line of business, said this partnership signifies a turning point in OT & cybersecurity.

"OT & cybersecurity are matters of national security, which mean greater responsibilities and commitment to our customers. Therefore, getting someone deeply specialised in the OT domain, like Oregon, adds excellent value for our customers and we expect this to add momentum to our growth and diversification," he said.

Naman Taldar, Regional Channel Manager at Oregon Systems, said the company's USP is its specialised niche



and highly experienced team.

"Ours is a purely channel-driven organisation and does not do business directly with the customers. Oregon Systems is purely an OT security distributor and our focus is mainly on ICS-cybersecurity. Our domain is very well-defined and we are the masters of it. Eight out of ten critical infrastructure clients in the region are already our customers because of the vendors in our portfolio. All these vendors complement each other. At Oregon Systems, we have developed a Zero-Trust architecture which has already been approved by most of the OEM vendors. Also, it has already been implemented in most of the critical infrastructure clients in the Middle East."

"Our technical team is highly skilled at what they do. Our engineers are the backbone of our business and they are IEC 62443-certified. They are well aware of the day-to-day challenges which a customer faces in the organisation in order to comply with industry standards. Hence, Oregon Systems is a frontrunner in the ICS/OT systems space," he added.

Arun George, SecOps Sales Lead, Emerging Markets, CyberRes – A Micro Focus line of business, stated that

THIS PARTNERSHIP SIGNIFIES A TURNING POINT IN OT & CYBERSECURITY.

customers in the OT space can greatly benefit with a partnership with them.

"At CyberRes – A Micro Focus line of business, we strengthen our customers' cyber resilience by delivering insights. protection, and compliance combined with security analytics. Specific to the Operational Technology space, which supports the critical infrastructure of the nation, we already have existing customers and we help them prepare for, respond to and recover from cyber threats - thus ensuring both cyber and business resiliency. OT/ICS has five levels of critical infrastructure and our technologies monitor each of these levels to provide real-time information to customers as well as integrate natively with other OT/ ICS security solutions," he added. 1

# AUTOMATING SECURITY



LEON WARD, VP OF PRODUCT MANAGEMENT AT THREATQUOTIENT, TELLS ANITA JOSEPH THAT 2022 WILL BE A BUSY YEAR FOR THE COMPANY AS IT FOCUSES ON BRINGING TO THE MARKET AN INNOVATIVE USER EXPERIENCE FOR CUSTOMERS TO I FVERAGE ITS APPROACH TO AUTOMATION.

hreatQuotient has
consistently been at the
forefront of innovating and
delivering what the SOC of
the future needs. Tell us
all about it.

The SOC of the future is built on data. and teams have never had greater access to it. While the data available from the various technologies, threat feeds, and other 3rd party sources is essential for threat detection and response, teams can quickly become overwhelmed by the volume of data, if care is not taken to properly manage it. ThreatQuotient has lived deep in this world of diverse security data, helping our customers manage this challenge, by improving their ability to understand and respond to threats by integrating their defences and processes at a data level, rather than at just a process level.

You recently announced V5 of the ThreatQ platform. What are the new additions/feature enhancements?

There are three main areas of enhancement. Firstly, Updates to the

DataLinq Engine. DataLinq is at the core of everything ThreatQ does, it performs the processes of ingest, Normalisation, Correlation, Prioritisation, and Translation of data. It does this so it can better connect those valuable dots that exist in your existing security data stores, and also between them. In version 5 (V5) specifically, our customers will notice a marked acceleration of how quickly data appears in the Threat Library, along with improved handling of object modification timestamps. This improvement has been

IF YOU THINK OF
HOW AUTOMATION
TOOLS HAVE EVOLVED
THROUGH DIFFERENT
USE CASES IT'S EASY
TO UNDERSTAND
HOW WE GOT TO THE
PROCESS DRIVEN
APPROACH

achieved though large changes in our approach to storing and processing data in the back-end. In addition to these brand new back-end changes, we're announcing some capabilities that we actually made available to our users over recent months. Smart collections is our new approach to allowing customers to define reusable sets of data across different use cases, from choosing what information is best reflected in a dashboard, identifying the correct threat indicators to operationalize, to building lists of prioritised events, Smart Collections will be the one-stop interface. Lastly, our ThreatQ Data Exchange module (TQX) is updated to allow better control and inclusion of related intelligence data.

#### A lot is being said about data-driven security. What are the advantages of this approach?

We're big proponents of data-driven automation here at ThreatQuotient, most importantly because it provides an approach that is better suited for automated detection and response

than the traditional process-centric implementations.

If you think of how automation tools have evolved through different use cases it's easy to understand how we got to the process driven approach. Think about the automation needs that have existed for IT or cloud system provisioning, or the QA (quality assurance) automation needs where a process is built to accelerate a series of the same tests or actions in a product or code. These automation needs have something in common, they know what they need to achieve when they start the process. This is not the same for security investigation and analysis processes, you never know where an investigation will take you before you start it. It turns out that the difference is fundamental.

This key difference of not knowing your target outcome when you start means a system has to learn as it performs its actions, generating a feedback loop to better guide execution. This is the foundation of what we call data-driven automation.

## How, in your opinion, is the cybersecurity landscape shaping up in 2022? What are the main trends?

We're seeing security operations technologies continue down on their convergence path, and automation has become a critical component within any scalable security strategy for good reason; Security teams are under constant pressure to do more. It's widely accepted that detection and response times are too high, and with the clear lack of available cybersecurity skills in the workforce, it's impossible to simply throw more manpower at the problem.

Automation of traditionally manual processes is seen as a way to unburden people from actions that may be considered a bad use of their time. If



you're looking for proof of this, just look at our QA automation team here at ThreatQuotient. When it comes to the SoC and security operations, why have people clicking buttons, copy pasting information between products, and performing other mundane tasks that don't leverage the security domain knowledge that they've been hired for.

## What will the focus of your security strategy be, this year?

This is lining up to be a busy year for

all of us here at ThreatQuotient! Our product strategy for 2022 is to continue on the path that we've started on with ThreatQuotient v5, and bring to market an innovative user experience for our customers to leverage our approach to automation. We've built out a lot of the data foundations for our vision already, and we're excited to close the loop by releasing the new user experience elements to disrupt how complex, or rather simple, data-driven automation can be. \$\frac{1}{2}\$



ver the last year, we have learned that there's no such thing as a predictable routine. Even as UAE authorities do their utmost to prevent the spread of the coronavirus, once-mundane everyday schedules can easily be disrupted by abrupt school closures, sudden quarantines or even an endless procession of deliveries of all kinds. At times when it can all get a bit too much, an extra layer of security can offer peace of mind.

But when you can't bring in new household help with visa and travel restrictions, technology can do your bidding instead. Indeed, technology is now so far advanced that with a couple of installs and a few quick tweaks, you can protect your home inside and out. With a video doorbell, indoor cameras around the house, and an app, you can create a ring of security around your home in minutes. When you choose a single brand of products, such as Ring, the devices can easily "talk" to each other, and best of all, everything can be monitored from your smartphone – even if you happen to be elsewhere physically.

As UAE residents have become more alert to visitors and the risks accompanying them, convenience and safety are more

important than ever. This is where Ring's bouquet of products can help.

#### Video doorbells help everyone

Since they were first created in 2013, video doorbells have proved their worth repeatedly in many different situations around the world. From a bear trying to open a car door to meteors flying through the skies, they have captured a number of untoward and unwanted visitors around the world. In some countries, law enforcement are even using doorbell video cameras to solve crimes.

Products such as the Ring Video
Doorbell 3 are activated by motion around
your front door and begin recording events
within their line of sight. Because Ring
video doorbells connect to the internet via
your home Wi-Fi system, this video feed
can be set to be livestreamed straight to
your phone, or you can access it later.

Even if you are at home, there is no need to go to the door. You can see who your visitors are from your smartphone. With the Ring Video Doorbell 3, you simply tap on the push notification to check who's at the door and even communicate with them. Even if you are at home, you can safely keep your distance from visitors, and if necessary, ask them to leave packages at your door.

#### Indoor cameras offer peace of mind

Meanwhile, for family-focused people who are away in the office or at an event outside the home (perhaps even in another emirate!), an indoor camera provides the assurance that no untoward incidents have taken place at home. Perhaps you want to chat with those who are at home, verify if your teenage kids are getting to their homework, or if your cat has been playing up while you're away.

A quick check is easy with a compact indoor camera such as Ring's Indoor Cam, which slots unobtrusively into small spaces around the home. This clever new device makes it easy to speak with older family members or see if school children have reached home.

Between the indoor cameras and the outdoor doorbell camera, you can easily keep an eye on every corner of your home from anywhere. In addition, with Ring's Protect Plan, it's easy to add an extra layer of security to your home. The number of cameras you cover depends on the plan you choose.

Although life has become more challenging on so many fronts, technology can help the stresses of living through these strange times. A little planning and a few moments' work can go a long way to securing peace of mind for everyone at home.

## Experience SELF-OPTIMIZING Wi-Fi, powered by Al



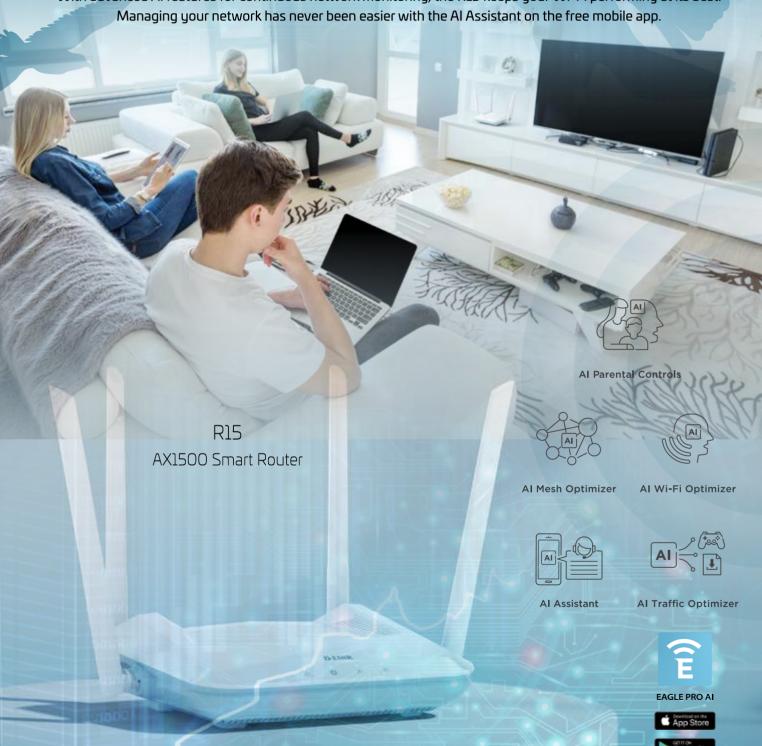
One Connection - Infinite Possibilities





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

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



# **XDR IN THE SPOTLIGHT**

TRELLIX IS A NEW CYBERSECURITY POWERHOUSE THAT HAS EMERGED FROM THE PREVIOUSLY ANNOUNCED MERGER OF MCAFEE ENTERPRISE AND FIREEYE IN OCTOBER 2021. IT PLANS TO DELIVER EXTENDED DETECTION AND RESPONSE (XDR) TO ORGANISATIONS WITH A FOCUS ON ACCELERATING TECHNOLOGY INNOVATION THROUGH MACHINE LEARNING AND AUTOMATION.

**ADAM PHILPOTT,** CHIEF REVENUE OFFICER AT TRELLIX, SPOKE TO **ANITA JOSEPH** ABOUT HOW THE NEW COMPANY IS ALL SET TO DELIVER ITS BRAND PROMISE OF BUILDING RESILIENT AND CONFIDENT ORGANISATIONS THROUGH 'LIVING SECURITY,' WHICH REFERS TO SECURITY TECHNOLOGY THAT I FARNS AND ADAPTS TO PROTECT OPERATIONS FROM THE MOST ADVANCED THREAT ACTORS.

ive us a background to this collaboration. If you think about it, there are a number of opportunities that go untapped in the industry today. Organisations continue to use technology to enhance their business, drive growth & efficiencies and also improve the way they interact with their clients using digital technology. We see this trend not just continuing, but also accelerating-with the new hybrid working patterns with distributed staff, we see newer and newer ways of reaching out to people in this virtual, distributed world-so digitisation continues to evolve and change shape.

What that means for our clients is that technology is an increasing part of how they do business. All companies are technology companies now. But what it also means then, is that the platforms that they're using to do business are digital and are increasing in complexity, which is giving rise to risk in the cyber domain. So then evermore digital, their attack footprint is greater, their attack surface is greater. Therefore cybersecurity becomes an increasing risk for them. So we need to help them with that.

At the same time, the platforms itself that they used to run their business are

growing ever wider-cloud technologies, mobile devices, home networks-all sorts of things that they need to try and put a security wrap around-and it's getting increasingly complicated. Then again, the way they try to secure is also complex. So, it's not only about a complicated digital platform, it's also about the fact that have invested in lots and lots of different security technologies over the years which has given rise to this massive complexity. And when you have so many different security tools, you need a lot of staff to operate them- to look at each tool, how it integrates, what information it's telling them, and so onand then to do correlation and respond to events that they see as they do this correlation. That complexity then drives

XDR IS PROBABLY
THE HOTTEST SPACE
FOR OUR CLIENTSIF YOU LOOK AT THE
DATA, THERE'S A
HUGE XDR MARKET
BUT IT'S MASSIVELY
UNDER PENETRATEDNOBODY'S OWNING IT
AT THE MOMENT.

a massive demand on human capacity which is slower than digital technology and also extremely expensive. So, managing complexity is something else that we need to do whilst augmenting the limited staff that they have. And then finally, as the threats themselves continue to increase both in volume and in sophistication-scaling this operation, particularly in light of that changing digital technology and that complex security environment, also becomes a challenge that we need to help them with.

#### Why Trellix?

With Trellix, we've brought together two industry giants-but, I like to refer to it as Trellix standing on the shoulders of giants and allowing us to see further. What we found is that these problems that I talked about earlier are not being solved in the industry today. They're not being solved by organisations and vendors who are desperate to have the latest feature, or the latest products-products won't solve this, we need to take a more holistic systemsbased view and architecture to addressing this. And so our focus will be on the XDR- Extended Detection and Response. This basically means that we're looking across a whole variety, the telemetry, then unifying it, treating it as one system and

automating the correlation across all of those disparate parts.

Bringing all that stuff together as an architecture so that we can automate the visibility, the investigation, the detection and also make the response and orchestration while enriching it with analytics-that's exactly what Trellix is doing. The other thing about the brand is that we're taking a very different approach-there's loads of organisations out there that sell a product and want to sell product after product after product, but they actually only make this complexity worse. There's organisations that have different fear-based names, but what we see is that businesses need to take risks, they need to manage the risks they take, but they also need to digitise in order to thrive. So, our job is to actually provide living-security that evolves as the business evolves, and to treat that as an overall system that's completely integrated into their digital strategy. And so there really are three pillars as to how we do that: one is around having a capability that's constantly learning and constantly adapting, as the world does, just as living things do, just as their digital strategy and environment does as well. So constantly learning, benefiting from AI and machine learning and improving the way they secure themselves, even with things they haven't even seen before and looking at threats they're likely to face, predicting those, helping them stay secure.

The second pillar, after learning and adapting, centres around being both native and open. We've got loads of capabilities that we benefit from, from both McAfee and FireEye. But we won't solve those problems just by doing that. The other thing we do is open to applications, open to third parties in the cyber community, and open to the infrastructure we're protecting, so that they can truly integrate this stuff together in a unified way. And then finally, we don't just bring products to organisations, we bring capability and talent and expertise, so that when you think about expertise in threat



research and intelligence, we have a huge number of capabilities and resources in our organisation. So not just sitting on top of the platform but integrating into it is exactly where we're going, and using that to enrich the threat intelligence that we have in that system to help our clients.

#### Why is Trellix focusing so much on XDR?

XDR is probably the hottest space for our clients-if you look at the data, there's a huge XDR market but it's massively under penetrated-nobody's owning it at the moment. But it's more than just the market that is driving us. We need to go deeper: Why is the market so big? Why is it of primary interest to our clients? And we realise that it doesn't just solve a niche problem, it solves a super set of problems. No customer has too few security capabilities. They've all got too much complexity. At the same time, none of them have enough staff-so, we need to be much smarter about how we augment limited human capacity by using things like Al and machine learning. All of that is very

rich in XDR-those are exactly the sets of things it sets out to do. Plus, as a company, looking at where we've come from, we have so much of those capabilities. It's a really natural fit for us in order to help our clients.

## What's 2022 looking like for Trellix? What are you planning for the market this year?

All of those challenges that I spoke about earlier will continue to be priority, and then XDR will be our superset solution to addressing that. That's what we'll be focused on. We'll also be focused on innovating-we've brought a really strong team together for this organisation, we're still building access to the key roles within that team. So we're talking of a really, really strong business, but then we already have a significant number of customers and we're highly penetrated. So, continuing to serve those customers, bringing some quick wins to them in terms of those different complementary capabilities and bringing those together to help clients solve those problems, will continue to be our core focus. 1

# ORGANISATIONS FALL SHORT ON DATA PROTECTION WHILE BUDGETS RISE TO TACKLE MOUNTING CYBER SECURITY CHALLENGES



Anand Eswaran, Chief Executive Officer at Veeam (L) and Claude Schuck, Regional Director, Middle East at Veeam (R)

he disconnect between business expectations and IT's ability to deliver has never been more impactful, according to the Veeam Data Protection Trends Report 2022, which found that 89% of organisations are not protecting data sufficiently. Veeam Software, the leader in backup, recovery and data management solutions that deliver Modern Data Protection, found that 88% of IT leaders expect data protection budgets to rise at a higher rate than broader IT spending as data becomes more critical to business success and the challenges of protecting it grow in complexity. More than two-

thirds are turning to cloud-based services to protect essential data.

The Veeam Data Protection Trends
Report 2022 surveyed more than 3,000 IT
decision makers and global enterprises
to understand their data protection
strategies for the next 12 months and
beyond. The largest of its kind, this
study examines how organisations are
preparing for the IT challenges they face,
including huge growth in use of cloud
services and cloud-native infrastructure,
as well as the expanding cyber-attack
landscape and the steps they are taking
to implement a Modern Data Protection
strategy that ensures business continuity.

"Data growth over the past two years

[since the pandemic] has more than doubled, in no small part to how we have embraced remote working and cloudbased services and so forth", said Anand Eswaran, Chief Executive Officer at Veeam. "As data volumes have exploded, so too have the risks associated with data protection; ransomware being a prime example. This research shows that organisations recognise these challenges and are investing heavily, often due to having fallen short in delivering the protection users need. Businesses are losing ground as modernisation of 'production' platforms is outpacing their modernisation of 'protection' methods and strategies. Data volumes and platform diversity will continue to rise, and the cyber-threat landscape will expand. So, CXOs must invest in a strategy that plugs the gaps they already have and keeps pace with rising data protection demands."

#### The data protection gap is widening

Respondents stated that their data protection capabilities cannot keep pace with the demands of the business, with 89% reporting a gap between how much data they can afford to lose after an outage versus how frequently data is backed up. This has risen by 13% in the past 12 months, indicating that while data continues to grow in volume and importance, so do the challenges in protecting it to a satisfactory level. The key driver behind this is that the data

#### **2922**

### **Top Trends in Data Protection**

Impact, costs, and benefits of modern data protection

In late 2021, an independent research firm surveyed over 3 000 IT decision makers and IT professionals about their IT and data protection drivers and strategies heading into 2022.

protection challenges facing businesses are immense and increasingly diverse.

For the second year in a row. cyberattacks have been the single biggest cause of downtime, with 76% of organisations reporting at least one ransomware event in the past 12 months. Not only is the frequency of these events alarming, so is their potency. Per attack, organisations were unable to recover 36% of their lost data, proving that data protection strategies are currently failing to help businesses prevent, remediate and recover from ransomware attacks.

"As cyberattacks become increasingly sophisticated and even more difficult to prevent, backup and recovery solutions are essential foundations of any organisation's Modern Data Protection strategy," said Danny Allan, CTO at Veeam. "For peace of mind, organisations need 100% certainty that backups are being completed within the allocated window and restorations deliver within required SLAs. The best way to ensure data is protected and recoverable in the event of a ransomware attack is to partner with a third-party specialist and invest in an automated and orchestrated solution that protects the myriad data centre and cloud-based production platforms that organisations of all sizes rely on today".

## Businesses face a data protection

To close the gap between data protection capabilities and this growing threat landscape, organisations will spend around 6% more annually on data protection than broader IT investments. While this will only go some way to reversing the trend of data protection needs outpacing ability to execute, it is positive to see CXOs acknowledge the urgent need for Modern Data Protection.

As cloud continues its trajectory to becoming the dominant data platform, 67% of organisations already use cloud



89% data loss and how IT

25% of organizations will change backup solutions for cost reasons, while 20% are looking

#### **Top Drivers** & Reality Gaps

It's increasingly common for "production" to outpace "protection," creating a gap between what businesses expect and what IT can deliver.





#### **Cloud Production** & Protection

Modernizing in 2022 usually includes an increase in cloud services for production and protection



center (physical and virtual), while 49% are cloud hosted

cloud services as part of their data protec





#### Ransomware Frequency & **Impact**

Ransomware is a disaster and an almost guaranteed threat that every organization must prepare for.

#### **Enterprise** & BC/DR

The keyword for 2022 for modernizing data protection is "heterogeneity." Organizations should be integrating their tools, automating processes, and orchestrating workflows





of IT leaders consider hybrid-cloud workload protection as the most important aspect of enterprise backup

#### **#1 Backup and Recovery**

that deliver Modern Data Protection, providing a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments.





services as part of their data protection strategy, while 56% now run containers in production or plan to in the next 12 months. Platform diversity will expand during 2022, with the balance between data centre (52%) and cloud servers (48%) continuing to close. This is one reason 21% of organisations rated the ability to protect cloud-hosted workloads as the most important buying factor for enterprise data protection in 2022 and 39% believe laaS/SaaS capabilities to be the definitive attribute of Modern Data Protection.

"The power of hybrid IT architectures is driving both production and protection strategies through cloud-storage and Disaster Recovery utilising cloud-hosted infrastructure," concluded Allan. "The benefits of investing in Modern Data Protection go beyond providing peace of mind, ensuring business continuity and maintaining customer confidence. To balance expenditure against strategic digital initiatives, IT leaders must implement robust solutions at the lowest possible cost".

Other key findings from the Veeam Data Protection Trends Report 2022 include:

- Businesses have an availability gap: 90% of respondents confirmed they have an availability gap between their expected SLAs and how quickly they can return to productivity. This has risen by 10% since 2021.
- Data remains unprotected: Despite backup being a fundamental part of any data protection strategy, 18% of global organisations' data is not backed up therefore, completely unprotected.
- Human error is far too common: Technical failures are the most frequent cause of downtime with an average of 53% of respondents experiencing outages across infrastructure/networking, server hardware and software. 46% of respondents experienced cases of administrator configuration error, while 49% were hindered by accidental

deletion, overwriting of data or corruption caused by users.

• Protecting remote workers: Only 25% of organisations utilise orchestrated workflows to reconnect resources during a disaster, while 45% run predefined scripts to reconnect resources running remotely in the event of downtime and 29% manually reconfigure user connectivity.

"FOR BUSINESSES
IN THE MIDDLE
EAST TO WIN THE
RANSOMWARE BATTLE,
THEY MUST POSSESS
THE CAPABILITY
FOR EDUCATION,
IMPLEMENTATION AND
REMEDIATION."

#### • Economic drivers remain

**critical:** When asked about the most important factors when purchasing an enterprise data solution, 25% of IT leaders are motivated by improving the economics of their solution.

#### Commentary and insights from Claude Schuck Regional Director, Middle East at Veeam Software

"The UAE and Saudi (the two biggest IT markets in the Middle East) findings of the Veeam Data Protection Trends Report 2022 largely mimics the global results, which find that the gap between business expectations and IT delivery, when it comes to data protection, continues to widen and has never been worse. As the proportion of applications that organisations consider mission-critical increases, so too does the volume and variety of cybersecurity threats. Entire industries face a data protection emergency and businesses across the world are looking for ways

to accelerate their strategies to protect data, remediate cyber-attacks and recover from systems outages."

"To be fully transformative. Middle East enterprises need to be anchored with key technologies provided by virtualisation, hybrid cloud and Kubernetes. Companies who succeed in accelerating their adoption of a Modern Data Protection strategy will put in place solid foundations to gain competitive advantage from digitisation. It will enable them to experience the lower cost points and flexibility of public cloud, leverage the security and proximity of private cloud, and fast-track their development cycles by deploying Kubernetes, with the assurance that their data is protected across their entire infrastructure".

"For businesses in the Middle East to win the ransomware battle, they must possess the capability for education, implementation and remediation. The best remedy for a security breach is prevention. This can be improved through education of employees, ensuring that cyber-attackers are not being gifted access to the data and systems they need to initiate a ransomware attack. The next strategy is implementation: offsite and offline backups to mitigate the effects of ransomware. Veeam advocates the 3-2-1-1-0 rule. There should always be at least three copies of important data, on at least two different types of media, with at least one off-site, one offline, with zero unverified backups or backups completing with errors. Finally, businesses need a plan for remediation. Do not pay the ransom. The only option is to restore data. Implementing a full Backup and Disaster Recovery plan gives organisations the ability to recover data in event of a ransomware attack. minimising the risk of financial and reputational damage".

The full Veeam Data Protection Trends Report 2022 is available for download at www.veeam.com/data-protection-report-2022.

#### 10TH EDITION

معرض و مؤتمر الخليج العالمي لأمن المعلومات



GISEC

GLOBAL

21 - 23 MARCH 2022 | DUBAI WORLD TRADE CENTRE

ARAB WORLD'S UNRIVALLED

CYBERSECURITY BUSINESS EVENT

GISEC is the ideal cybersecurity platform to participate & partner with vendors and government entities in the region.

H.E. Dr. Mohamed Al-Kuwaiti, Head of Cyber Security, United Arab Emirates Government

**ENQUIRE ABOUT EXHIBITING, SPEAKING AND SPONSORSHIP** 

971 (04) 308 6267 | gisec@dwtc.com | #GISEC

OFFICIALLY SUPPORTED BY

OFFICIAL GOVERNMENT CYBERSECURITY PARTNER

OFFICIALLY SUPPORTED BY











OFFICIAL DISTRIBUTION PARTNER







STRATEGIC PARTNERS

ORGANISED BY



# REDEFINING DATA STORAGE

Jermaine Campbell

ANITA JOSEPH, EDITOR, SECURITY
MIDDLE EAST, CAUGHT UP
WITH **JERMAINE CAMPBELL**— HEAD
OF VIA SALES, EMEA AT SEAGATE, TO
FIND OUT HOW THE COMPANY IS
HELPING THE MARKET FAST TRACK ITS
DIGITAL TRANSFORMATION JOURNEY
WITH ITS CUTTING-EDGE PRODUCTS
AND SOLUTIONS.

ow would you
describe Seagate's
presence in the region?
What has the journey
been like, so far?

We've been in the Middle East for a long time, it's been a memorable journey. We've had our ups and downs, but I sense great stability from a brands perspective, and also from a resource and headcount perspective. Also, the response that we got from the recently concluded Intersec 2022 also shows an appetite from businesses here in this market, to engage with Seagate and to partner with us. So I would describe our presence right now as filled with opportunity and great potential to grow and to develop. People recognise our brands and are ready to engage with us.

# What were the main learnings now of 2020? Particularly post the pandemic everyone's been, in survival and growth mode-how did Seagate keep up with the challenges?

I think the main learnings for 2020 were around the durability of the market. Despite the pandemic, people were actually able to go ahead with business, although it was difficult, and they needed several changes to be made.

We saw, for instance, that for cash flow purposes, people moved to more entry level applications and left the door open for upgrades later on, in order to keep their business moving. At the same time, people were also ready to adopt new technology to address some of the health and safety concerns around COVID. I'm specifically talking about thermal cameras and thermal camera technology. And how did that affect us on HDD? You know, a lot of these cameras required or have Al capability. And the resellers-installers were much more open and interested in how our AI drives were able to support these kinds of Al applications.

## How is Seagate supporting the data market with its resources and technology?

The total data sphere is growing at really astronomical rates. In fact, the amount of data being created in the world is doubling every three years, which is incredible. But what is really driving that growth is the surveillance market-and that's coming from high resolution cameras. It's coming from people not just wanting to record data for surveillance purposes, but also for like business insights. It means that they're retaining the data and keeping it for analysis longer. This requires a kind of higher capacity and different types of storage.

So I think Seagate right now as a as a data storage-centric company, is really

set to support this market with the right technology and the right portfolio-right from the edge to centralised storage. The Middle East is really leading the world when it comes to the surveillance market, whether it be smart city or smart road applications. So, the support that we offer here in the Middle East is really going to be critical for Seagate in 2022. One of the things that we've done is that we've launched an application on mobile phones, where the installer can register/login and get hold of quick information on storage calculators or compatibility guides, or creating warranty claims and so on.

Also, if the drive is damaged, due to a fire or an explosion, for instance, Seagate is offering a free-of-charge data recovery service, which can have a value of anywhere around \$300 to \$500. This is an in-house service, provided by our own Seagate laboratories, and is a safe and secure way of recovering the data in case you have footage that you that you need to recover and provide to the police for evidence. So, this is another exclusive value add that Seagate is offering in this competitive market. Therefore, having a close engagement with Seagate in this market is really critical and that's what we're responding to, in 2022.

THE TOTAL
DATA SPHERE IS
GROWING AT REALLY
ASTRONOMICAL
RATES. IN FACT, THE
AMOUNT OF DATA
BEING CREATED
IN THE WORLD IS
DOUBLING EVERY
THREE YEARS.

# That brings us to Seagate's flagship products. Can you tell us tell us more about them-particularly the surveillance range of products?

Yeah, so we bring to the market surveillance storage, right from the edge to centralised storage. So we start from the edge and have entry level DVRs and NVRs. We've positioned our SkyHawk drives-these go from 1 TB to 8 TB

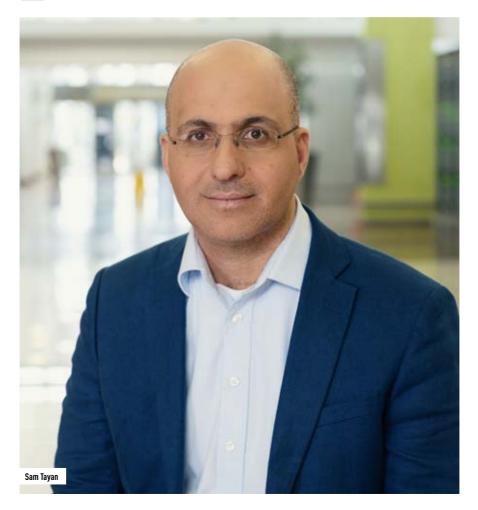
For more Al-intensive applications, heavier workload, higher camera counts and applications, we've got our SkyHawk Al drives and these start at 8 TB and go up to 18 TB. That's from a device perspective, but I think what's been really interesting is the interest shown with Seagate's centralised storage and Sand solutions that we brought to the market, which offer the fastest data transfer rates and the highest density for capacity storage.

### What is your outlook for the market for 2022?

Specifically for this Middle East region. there's so much opportunity, and I'm not just talking about physical units and revenue, I'm talking about partner engagements. We have our partner program where partners are able to actually get closer to us and learn about our products- we've got regular courses that they can take to learn about how storage fits into the surveillance market, and how to use latest technology and some of our new services as well, that we provide in the market, like data recovery, which we branded the Seagate rescue. So, how do you engage with Seagate to present your marketing plans and demonstration products? This is all done by our partner program. So, that's a real big outlook as well as opportunity, for us to increase our sales and revenue in the region. 🙎

# DRIVING DIGITAL COMMUNICATION

ANITA JOSEPH CAUGHT UP WITH **SAM TAYAN,** HEAD OF MENA AT ZOOM, TO FIND OUT HOW THE COMPANY'S DISCIPLINED APPROACH, FOCUS ON LONG-TERM SUSTAINABLE GROWTH AND PROVEN TRACK RECORD OF INNOVATION CONTINUES TO DELIVER HAPPINESS TO CUSTOMERS AND EMPLOYEES



ow much has video communication evolved, especially in the last two years since the onset of the pandemic?

While we've all been relying on video communications for the better part of the past two years, these technologies have transformed and adapted to the changing circumstances, accommodating the new modes of flexible work, blended learning, and hybrid events. However, as we approach recovery and return to life as we know it, this vital industry will not be left behind.

We've added additional features to our core unified communications solution to give customers everything they need to support digital and hybrid workplaces, including:

- Zoom Phone end-to-end encryption and video voicemail.
- Enhanced whiteboard, an interactive collaboration feature, now with VR functionality through Oculus, allows teams to collaborate as if they were in person.
- Live translation and transcription to allow seamless collaboration for all.
- Interactive maps and authentication for hot-desking, a bridge between virtual and in-person.

- Zoom Chat features like huddle room and widgets to enable workplace community from anywhere.
- Zoom Rooms The modern workspaces for hybrid teams, Zoom Rooms bring HD video collaboration into any space in the office, in the classroom, or at home and enable in-person and remote participants to interact in real time
- Zoom Events Conference empowers hosts to organise multi-track and multiday events in a sophisticated format, with rich functionality, including event lobby, chat, networking, sponsors, surveys, recordings, analytics, and more.
- Zoom Apps are built to optimise meeting workflows and will be made available throughout the platform, including Zoom Apps for Webinars and Zoom Apps for Mobile, as well as immersive apps, which will enable even more productive and collaborative app experiences.

#### What does the common criteria benchmark recognition mean for Zoom in its journey? What can users look forward to?

This Common Criteria certification represents a major milestone for Zoom as we are the first video communications client to receive this important certification, reinforcing our commitment to our customers.

Security and privacy are the cornerstones of everything we do, and we are continually innovating secure solutions for all users of our platform.

# Work transformation continues to be one of the biggest challenges business leaders are faced with today. How is Zoom stepping in to help them redefine the employee experience?

As we enter a new era for communications and collaboration,

"WE FOCUS ON
INNOVATION TO
BUILD OUR OFFERING
AT SPEED AND SCALE
- OUR ABILITY TO DO
SO CAN BE SEEN IN
THE SUCCESS OF OUR
DIFFERENT FEATURES
AND OFFERINGS."

there is a need for immersive video experiences that allow for a robust hybrid setup regardless of the industry. Zoom's disciplined approach, focus on long-term sustainable growth, and proven track record of innovation will continue to deliver happiness to their customers, employees, and communities.

In the UAE, most companies have adopted a hybrid work model and innovative work schedules, so video communications will continue to be crucial.

We focus on innovation to build our offering at speed and scale – our ability to do so can be seen in the success of our different features and offerings, such as Zoom Phone, which has expanded to over 40 countries and sold over 2 million seats. We believe our global brand, innovative technologies, and large customer base position us well for the future.

Our vision is to empower people to accomplish more. We aim to empower professionals, so they can serve their clients, serve their companies, serve their people.

#### What are your plans for 2022?

Zoom has big plans to continue providing solutions and services that streamline digital communication and contribute to the hybrid work environment. This year, we are planning the launch of new features in as:

- Huddle view: Huddle view will provide you a visual picture of a channel, providing teams a sense of togetherness while they communicate and collaborate, bringing your dispersed teams together in a digital area.
- Zoom Events Backstage: Speakers, panelists, and production staff can use Zoom's backstage feature to reply to questions, monitor chat, and mingle before going live.
- Zoom Whiteboard: The all-new Zoom Whiteboard allows on-site and remote participants to engage in real-time on a persistent digital whiteboard from any location and at any time. The new Zoom Whiteboard can be used in any Zoom Meeting.
- Zoom Widget: Zoom is developing the Zoom Widget to help you get an instant glimpse of your meeting calendar, check who is already in a meeting, send a brief chat, and more.
- Zoom Apps for Mobile and Webinar: Zoom Apps are now available for the Zoom mobile app as well as Zoom Video Webinars. Zoom will also release Immersive Apps, which will allow you to customise your Immersive Views.
- Video Engagement Center: The Video Engagement Center will be a straightforward, cloud-based solution that allows you to connect professionals and end customers over video, with the same cloud-first scalability and trusted video architecture you've come to expect from Zoom.
- Enhanced translation and transcription: Zoom is adding live translation and expanding its autogenerated captioning to support a range of languages in the coming year.
- Jumpstart by Zoom: Zoom is working on Jumpstart, a new app builder tool that will help developers get their apps to market faster by providing industry-leading, dependable video.



n 2021, we observed a resurgence of enterprise ransomware with a shift towards larger organisations. By attacking enterprises with a larger reach, threat actors are looking to increase their financial gains without increasing effort. The rise of ransomware attacks on supply-chain and third parties is resulting in 'one-to-many' compromise.

On average, enterprises have approximately 5800 vendors they depend on for business functionality, and 20% of these pose a high risk. Since third-party (and fourth party) cybersecurity is often not up to the mark, and there is a lack of visibility of real-time cyber risk the third parties pose to a business, cybercriminals are targeting third-party vendors to laterally breach multiple larger organisations simultaneously.

In 2022, ransomware is evolving; sensitive credentials will be stolen and leaked without any waiting period, customers' data will be exposed and customers will be directly threatened. Therefore, reactive techniques and reliance on data backups alone wouldn't help. Organisations will have to proactively prepare for ransomware

attacks and have dedicated playbooks in place to manage and mitigate them.

#### Managing ransomware proactively

Firstly, an organisation should define what financial risk they are facing as a result of ransomware attacks; it varies depending on the geography, industry, and size of the business. Once they have calculated this value, they must build a strategy to accept, reduce or transfer the risk.

If the damage is within acceptable limits, the business should focus its efforts on other facets of its cybersecurity strategy. However, to reduce the financial impact, they can either purchase cybersecurity products/services to improve their cyber risk posture or patch identified vulnerabilities. The problem is that in today's dynamic and digitally native businesses, there are over 40-50 cybersecurity products/services; each with its dashboard, warnings, and priorities. Cybersecurity teams are often overwhelmed and miss important SOC alerts that could potentially warn about ransomware attacks.

Businesses should understand that more cybersecurity products does not

mean better security. A shift in mindset will enable businesses to move towards a predictive approach where signals from various cybersecurity services - are unified and integrated in real-time, using ML-enabled risk assessment techniques to quantify the cyber risk posture across all vectors (people, processes, and technology for 1st and third-party). A single dashboard approach that helps businesses measure, manage and mitigate threats such as ransomware and others will aid CISOs and security teams to have a proactive view of what's going right and what can be better; with a contextual understanding of the direct financial impact of every cybersecurity initiative undertaken to reduce the risks.

Lastly, a part of the cyber risk can be transferred via cyber insurance and in 2022, we will see a rise in mandatory cyber insurance to have a baseline level of protection, especially for businesses in critical sectors such as FinServ, Healthcare, Power, etc. No organisation can be 100% secure but they can be 100% prepared. Cyber risk quantification makes cybersecurity simple, dejargoned, and contextual by improving visibility of cyber risk.



# SECURE BY DESIGN

Leading the Way to Safer IT

Secure by Design guides our delivery of powerful, affordable, and secure solutions. We're confident our actions will create the most secure and high-quality software in the industry.

















# Solar Powered Camera



Powered by solar energy, this kit sets up without any electrical wiring.

## **Easy installation**

Easy set up without mechanical equipment-reducing the installation costs and time.

Can withstand bad weather

Prone to extreme weather such as strong wind and rainstorms.

