ISSUE 52 | NOVEMBER 2020 WWW.TAHAWULTECH.COM





EXPERT'S CORNER:

TECHNOLOGIES' MICHEL NADER

VEEAM: 3 STEPS TO **BOOST SECURITY** FOR THE HYBRID **BUSINESS**



ROHIT BHARGAVA

RESHAPING SECURITY

HOW CLOUD BOX TECHNOLOGIES IS DELIVERING BESPOKE SOLUTIONS TO PROTECT ENTERPRISES AS THEY ADVANCE THEIR DIGITAL JOURNEYS IN THE NEW NORMAL



RAQMIYAT'S

BEYONDTRUST'S HATHAWAY



SUPPLEMENT



HUAWEI CLOUD Grow with Intelligence

Launch in Middle East in November 2020





CONTENTS

Securaty









Reshaping security innovation

How Cloud Box Technologies is enabling secure digital journeys in the new normal

20 EXPERT'S CORNER

Dell Technologies: The right playbook to fight against ransomware

22 ACCELERATING CLOUD INNOVATIONS IN THE DIGITAL ERA

How cloud, cybersecurity and the channel can fast-track digital transformation

30 PROACTIVE CYBER DEFENCE, A KEY TO NATIONAL SECURITY

Why government firms must be prepared to tackle cyber-attacks that pose threat to national security and integrity

38 LAST TAKE
3 steps to boost security for the hybrid business



SD-WAN can deliver reduced WAN costs. But it can't be at the expense of Security.

Fortinet's Secure SD-WAN solution provides full SD-WAN capabilities with all of the Next Generation Security features needed for today's ever-changing threat landscape.



www.fortinet.com



EDITORIAL



Talk to us: E-mail: adelle.geronimo@ cpimediagroup.com

Adelle Geronimo Editor

EVENTS





SECURING FUTURE SUCCESS

SUCCESSFULLY

NAVIGATE THE

BOTTLENECKS.

HAVING

THE RIGHT

LEADERSHIP

WHETHER IT BE

FOR BUSINESS, IT

As the world continues to grapple with the new ways of interacting with people, new ways of doing business and unprecedented shifts in the economy, many are staying resilient and

What's even more encouraging is that we attack are seeing many businesses take today's order to unexpected challenges as an opportunity having to accelerate their digital transformation busine journeys. However, cybersecurity remains a key concern.

steadfast in adapting to the new normal.

Many threat actors are taking advantage of the uncertainties and fears surrounding the pandemic. In fact, consumers and businesses in the UAE suffered more than 600,000 phishing attacks over the last few months, according to findings by Kaspersky.

Additionally, another study by

Juniper Networks has revealed that
93% of Middle East firms admitted
to experiencing challenges when attempting to
secure their organisation's network effectively
as they cope with a distributed workforce.

OR SECURITY IS
FUNDAMENTAL.*

technological deemed to the neemble of the neemble o

This shows a clear narrative that having a security-aware workforce is vital and that the old way of thinking about security will no

longer suffice for those companies battling a new norm.

Looking ahead, we can expect more challenges as things remain uncertain due to the ongoing global health crisis. Cyberattacks can happen anywhere, anytime. In order to successfully navigate the bottlenecks, having the right leadership whether it be for business, IT or security is fundamental.

On that note, I am happy to announce that this month we will be hosting the CISO50 and Future Security Awards. The virtual event recognises individuals, businesses, and vendors that have successfully navigated today's challenges and thrived through digital technologies and delivered ground-breaking value through innovative application of security technologies. It acclaims the best security minds in the region whose

technologies, products or solutions are deemed to have a great potential in meeting the needs of today's new business normal. Please tune in on 24th November, 10AM (GST) as we celebrate excellence and leadership in IT security.

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

Published by



Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com +971 4 440 9139

ADVERTISING Group Sales Director Kausar Syed kausar.syed@cpimediagroup.com +971 4 440 9130

Senior Sales Manager Sabita Miranda sabita.miranda@cpimediagroup.com +971 4 440 9128 EDITORIAL

Editor
Adelle Geronimo
adelle.geronimo@cpimediagroup.com
+971 4 440 9135

Contributing Editor
Mark Forker
mark.forker@cpimediagroup.com
+971 4 440 9153

DESIGN Senior Designer

Analou Balbero
analou.balbero@cpimediagroup.com
+971 4 440 9140

DIGITAL SERVICES
Web Developer
Jefferson de Jova

webmaster@cpimediagroup.com +971 4 440 9100 Registered at Dubai Production City, DCCA PO Box 13700 Dubai. UAE

> Tel: +971 4 440 9100 Fax: +971 4 447 2409

Printed by Emirates Printing Press LLC, Dubai

> © Copyright 2020 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.

MIMECAST. **CROWDSTRIKE TEAM UP TO ENABLE CUSTOMERS BETTER DEFEND AGAINST THREATS**

PETER BAUER. MIMECAST

Mimecast

has joined the CrowdStrike Flevate Partner

Program, an elite cybersecurity ecosystem delivering solutions and expertise to stop breaches.

Through Mimecast partnering with CrowdStrike, customers can better defend against threats at the perimeter, inside an organisation and beyond, improving an organisation's overall security posture.

The CrowdStrike Falcon platform offers cloud-based architecture that is highly scalable in nature and secures all devices and workloads in real-time across an organisation. Complementary to Mimecast's defense approach, this integration expands community immunity exponentially helping to quickly identify and resolve incidents.

Through this partnership, customers' endpoints are enriched by email and web data along with indicators of compromise. The sharing of newly discovered threats and growing threat activity will improve customers' overall cyber resilience postures by helping avoid downtime and costly breaches.

Peter Bauer, chief executive officer of Mimecast, said, "Organisations need deep email threat intelligence that is integrated into their endpoint to make their systems work better together so the identification. prevention and response to threats are connected, orchestrated and automated. CrowdStrike was a perfect addition to our ecosystem of partners as the combination of endpoint, email and web security will offer Mimecast and CrowdStrike joint customers actionable threat intelligence to build a stronger cyber resilience posture."

HIPERDIST, KEEPER SECURITY PEN DISTRIBUTION DEAL FOR MEA

Hiperdist, one of the fastest-growing

IT solutions distributors in MEA, has announced a strategic alliance with cybersecurity company Keeper Security.

As part of the agreement, Hiperdist will distribute the complete range of Keeper products across the Middle East and Africa region.

"Robust, comprehensive cybersecurity solutions are the need of the hour. We are excited about this partnership. which will allow our partners to mitigate cyber-threats by preventing passwordrelated data breaches cyberthreats while reducing operational costs," said Roland Steinmetz, Director of Channel – EMEA at Keeper Security.

Keeper Security offers the only enterprise password manager that is built on a fully zero-knowledge architecture and that is ISO 27001 and SOC2 certified.

GOVIND HARIDAS, HIPERDIST



Govind Haridas, Business Head - Cyber Security at Hiperdist, said, "In the UAE alone, as many as 82% of organisations faced at least one cyber-attack in 2019. Poor password hygiene, mishandling sensitive information are some of the leading causes of such threats. Keeper Security focuses on password management and protection across businesses of any size - from startups to managed service providers to enterprises. We plan to leverage our deep reach in the region and decades-long expertise to support them, empowering our partners with their applications in the cybersecurity toolkit."

MCAFEE LAUNCHES SECURE CLOUD NATIVE APPLICATION ECOSYSTEM

McAfee has announced MVISION Cloud

Native Application Protection Platform (CNAPP), the industry's truly integrated architecture to secure the cloud native application ecosystem.

MVISION CNAPP delivers consistent data protection, threat prevention, governance, and compliance throughout the cloudnative application lifecycle, including container and OS-based workloads.

"Organisations want to unleash the creativity of their developers to rapidly develop and deploy compelling and compliant cloud-native applications that harness the power of the cloud," said Rajiv Gupta, senior vice president, Cloud Security, McAfee.

"But in order to do that they need an equally cloud-native platform to address the new security needs of this new

RAJIV GUPTA,

MCAFFF

environment, McAfee MVISION CNAPP extends MVISION Cloud's data protection - both Data Loss Prevention and malware detection - threat prevention, governance and compliance to comprehensively address the needs of this new cloudnative application world thereby improving security capabilities and reducing the Total Cost of Ownership of cloud security."

MVISION CNAPP is the industry's first platform to bring application and data context to converge Cloud Security Posture Management (CSPM) for public cloud infrastructure, and Cloud Workload Protection (CWPP) to protect hosts and workloads including VMs, containers, and serverless functions.

TENABLE UNVEILS NEW INNOVATIONS TO SWIFTLY PREDICT CYBER RISKS

Tenable has announced new Tenable

Lumin innovations that empower customers to align business objectives with cybersecurity initiatives.

The latest enhancements to the Cyber Exposure Management Platform enable organisations to predict which vulnerabilities pose the greatest business risk and act with confidence to effectively reduce risk across their modern. distributed environments.

As the performance of our global economy increasingly depends on the uptime and security of digital infrastructure, cyber risk has become inherent to business risk. But the modern attack surface has expanded with new assets — from cloud to IoT to operational technology — and CISOs struggle to understand their true level of exposure and address risk based on business priorities.

The following capabilities announced includes Remediation Maturity. Mitigations and Predictive Scoring. Tenable's predictive technologies



are powered by Exposure.ai, which continuously analyses 20 trillion aspects of threat, vulnerability and asset information with machine learning algorithms to predict critical exposure points before they can be leveraged in an attack.

TENABLE

"Technology investments are now powering our economy and have become central to our very way of life. Modern organisations require an innovative approach to cybersecurity — one that is holistic and predictive, not piecemeal and reactive, and most of all, aligned to the strategic priorities of the business," said Renaud Deraison, chief technology officer and co-founder, Tenable. "Lumin now allows our customers to properly assess and track their Cyber Exposure and the maturity of their processes. For the first time, they can evaluate the ROI of their investments towards remediation and mitigation and understand how they stack up against their peers."

FORTINET NAMED A LEADER IN THE 2020 GARTNER MAGIC QUADRANT FOR WAN EDGE INFRASTRUCTURE

Fortinet has announced it has been positioned in the Leaders quadrant of the Gartner September 2020 Magic Quadrant for WAN Edge Infrastructure, placing higher in ability to execute and further in completeness of vision than its position the previous year.

John Maddison, EVP of Products and CMO, Fortinet, said, "A few years back while the entire industry was thinking about SD-WAN as a siloed product, at Fortinet we took a Security-driven Networking approach, combining networking and security to be the first vendor to deliver Secure SD-WAN. We're

pleased to be placed in the Leaders quadrant of the 2020 Magic Quadrant for WAN Edge Infrastructure, something we feel is another strong indicator of Fortinet's ability to deliver better user experience with consistent security for our customers. We believe Fortinet will continue to disrupt the industry with solutions rooted in Security-driven Networking principles, next by delivering the most flexible security via SASE."

STARLINK ENHANCES IAM PORTFOLIO WITH SAILPOINT PARTNERSHIP

NIDAL OTHMAN. STARLINK

StarLink has announced

a partnership with SailPoint



Turkey. The joint objective is to help organisations drive business efficiency with a robust Identity Management

for distribution in the Middle East and

SailPoint delivers an innovative approach to securing access across enterprises with the SailPoint Predictive Identity platform, which is powered by AI and Machine Learning (ML) technologies.

The two companies, through this robust collaboration, will aim to empower enterprises in the region with advanced capabilities to help accelerate their business while delivering adaptive security, continuous compliance, and improved business efficiency.

"The impact of cybersecurity breaches is astounding, which calls for a Zero Trust approach. What customers need today is a strong Al-driven identity strategy that can enable efficient access without compromising on security or compliance. StarLink's solutions portfolio consists of very strong technologies within its Access Control domain and our alliance with SailPoint will further

> strengthen our offerings as it complements

> > with many of the Privileged Access Management (PAM) solutions," said Nidal Othman,

co-founder and managing director, StarLink.

OF ORGANISATIONS EXPERIENCED AN INCREASE IN ENDPOINT AND IOT SECURITY INCIDENTS IN THE LAST YEAR

www.tahawultech.com NOVEMBER 2020 7

NO MORE RANSOM!

Partners 163



Partners breakdown

Academia - 2%

Telcos **-■ 2%**

Consulting **→ 3%**

EU Agencies —■ 4%

Non profit / Public organisations — 6%

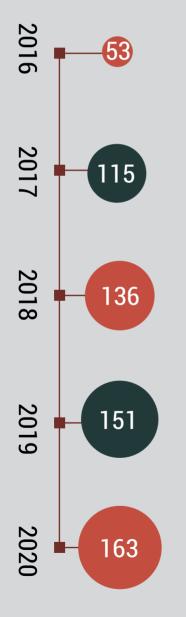
Financial services — 7%

CERTs — 11%

Law enforcement — 28%

Internet security companies — ■ 37%

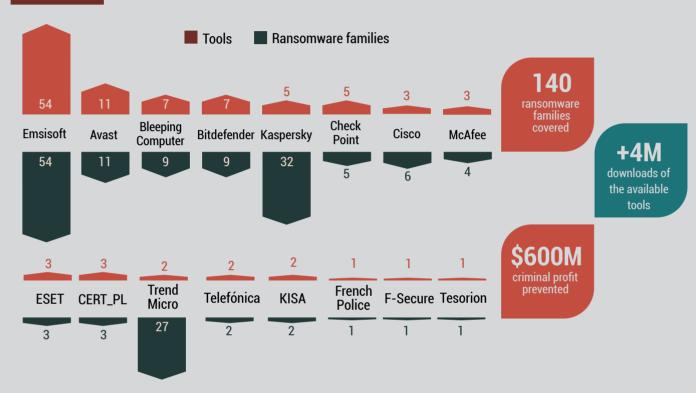
Partners annual growth



In July 2016, the No More Ransom initiative was launched by the Dutch National Police, Europol, McAfee and Kaspersky. Today there are 163 partners all over the world. The portal has added 28 tools in the past year and can now decrypt 140 different types of ransomware infections. The portal is available in 36 languages.

Celebrating its fourth anniversary, the No More Ransom decryption tool repository has registered over 4 million visitors from 188 countries since its launch and has stopped an estimated \$600 million in ransom demands from ending up in criminals' pockets.

Tools 110



Language & countries

Top 5 languages among 36 available

Top 5 countries of traffic



www.tahawultech.com NOVEMBER 2020

HIKVISION®

FIVE REASONS WHY SMBs SHOULD EMBRACE THE CLOUD FOR THEIR PREMISES SECURITY SOLUTION

THE CLOUD HAS EMERGED AS A MORE SCALABLE AND OPEN OPTION FOR BUSINESSES OF ALL SIZES, THE SECURITY INDUSTRY IS NO EXCEPTION. READ ON TO DISCOVER HOW THE CLOUD CAN MAKE PREMISES SECURITY OF SMALL AND MEDIUM-SIZED BUSINESSES (SMBs) MORE COST-EFFECTIVE, EFFICIENT, FLEXIBLE, SCALABLE, AND, ULTIMATELY, MORE EFFECTIVE WITH CONVERGENCE AND AUTOMATION.

ore and more businesses today are leveraging the cloud to improve business operations and management. In retail, for example, progressive retailers have been implementing cloud commerce solutions for their order management, inventory management, financial consolidation and customer relationship management (CRM).

Similarly, the physical security industry is embracing cloud in a big way. Cloud-based security systems – which bring together security, networking, storage, analytics and management – are increasing in popularity due to their impressive safety and operational benefits.

So, what exactly are the benefits of a security solution that's managed in the cloud? In this blog, we examine five reasons why cloud should be front of mind for SMBs for their premises security solution.

Security information at your fingertips: always

A cloud-based security solution enables businesses to access and manage all of their security devices anytime, anywhere, and on any internet-enabled device. And when businesses have multiple premises to manage, the cloud provides an easily accessible and secure collation point for information from all secured buildings. Managers can check live video and stored data from each location, even when they are travelling, as long as there is an internet connection.

Reduced upfront investment and easy setup

All businesses want platforms or services that offer simplicity, with as few assets to manage as possible, and a setup that's ultra-simple. This is precisely where the cloud delivers. Through a cloud hosting infrastructure, there is no need for a local

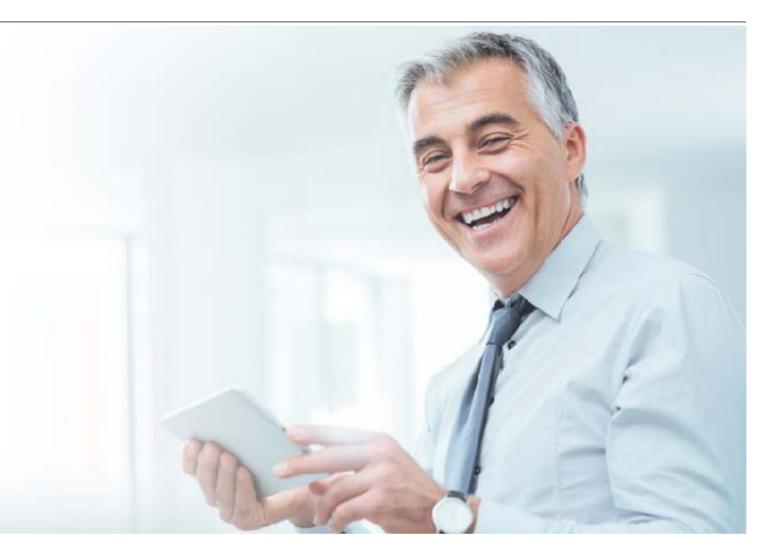
server or software to be deployed; to get started, all you need is a username and password, and you can easily connect devices like video cameras to the internet for preview and playback.

This is particularly useful for organisations with smaller/fewer sites and fewer cameras, as it helps to reduce the cost of hardware investment and ongoing management.

Scalability and flexibility

Scalability is one of the main reasons to migrate to the cloud. Whether traffic or workload demands increase suddenly or grow gradually over time, companies choose a cloud solution because it's scalable, allowing businesses to increase storage and performance appropriately and cost-effectively.

This is very much the case for cloud-based security solutions. When



businesses grow, the cloud enables their security system infrastructure to scale with it. Companies can add new devices, services, functionality and enhanced analytics and data storage in stages, to suit their growth and development.

Remote system maintenance 24/7

Cloud-based platforms can help to make managed security services far more responsive. Security service providers and alarm receiving centers (ARC) can constantly monitor the health of an end-user's security system and resolve any problems remotely, delivering a sophisticated service without the added expense of an on-site visit. All that's required is consent from end users when the system is deployed.

For businesses, this offers peace of mind that their security system is up and running 24/7. Any issues such as device

failure or communication loss can be addressed rapidly and efficiently.

Technology that's always up to date

Technology is always changing. So for onpremise systems, regular maintenance must be carried out on-site or through remote desktop. This can be a burden to IT services, especially if there are multiple sites.

A cloud-based solution, however, requires no on-site manual updates, as customers will stream the latest version of the software that is fully and centrally maintained by the service provider. This saves a significant amount of time, while reducing the potential of security lapses and the associated risks.

A convergent, cloud-based security service solution from Hikvision

Hikvision's cloud-based security service

solution, Hik-ProConnect, is designed for SMBs and residential applications. It uses industry-leading standards and protocols for maximum security and reliability, making it ideal for today's security market.

Incorporated with all these cloud-hosting benefits, Hik-ProConnect allows users to converge multiple devices into one management platform with a single login. This goes above and beyond conventional security systems made up of disparate elements. Integration of devices provides users with different types of events to suit their requirements, away from manual approaches to the use of automation. Examples of device linkage include merging intercom calls and intrusion or access events with video verification.

Whether being used to manage a single simple site or multiple complex locations, Hik-ProConnect ensures users enjoy an upto-date and smooth running security system.

www.tahawultech.com NOVEMBER 2020



and professional services catering to enterprises, government, BFSI, SMBs to name some. We offer end-to-end solutions for IT infrastructure, data management, information security and virtualisation. Our portfolio includes some of the best solutions for data centres, storage, server, back up, disaster recovery, network security, cybersecurity, desktop virtualisation as well as cloud including public cloud, private cloud and hybrid cloud.

We have a strong team of talented and qualified professionals, who work closely with our customers to put together a strategy after studying and evaluating their requirements. They, then, design, develop and implement systems and processes that help customers best achieve their digital transformation goals. CBT provides the perfect combination of value and expertise required to deploy the latest solutions for our clients.

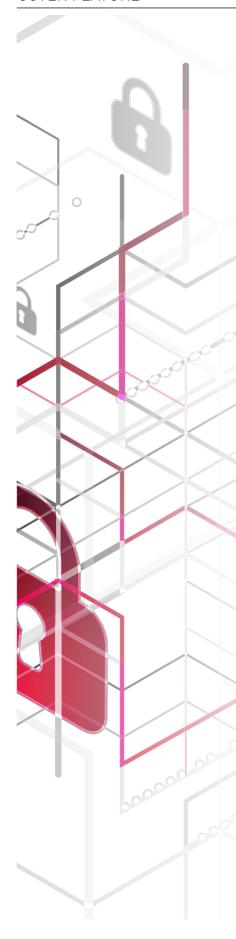
CBT is positioned to offer a single interface to technology integration and services and provides effective and efficient IT infrastructure sourcing and enabling services to organisations of all sizes across different industry segments. We offer integration of IT technologies to deliver business value to our customers. We have also made investments in network operation centres in Dubai and India as a part of our managed services.

A recent industry study has highlighted that the global hybrid cloud market is expected to generate \$171.93 billion by 2025. What are the key drivers behind this trend?

RB: Cloud is the primary platform for enabling digital transformation



www.tahawultech.com NOVEMBER 2020



Does having a multi-cloud or hybrid cloud approach result in organisations having to deal with multiple and more complexities? What kind of best practices can enterprises adopt to counter the challenges brought by these complexities?

RB: Enterprises choose to work with multiple cloud providers for a host of reasons such as staying competitive, taking advantage of best of breed offerings, avoiding medium- and longterm vendor lock-in, boosting data integration and data sharing across applications, and improving maturity of cloud governance and administration. The guidelines for building a multicloud portfolio of service providers is to check architecture, design, modularity, style, across the various players; compare availability, performance, data sovereignty, regulatory requirements, labour costs, of the cloud providers; assess governance, control, administration, monitoring, policies, procedures, processes, cost, optimisation, across the options; and check various service offerings like disaster recovery, migration of data, migration of applications, from the existing cloud service providers.

As enterprises scale their usage of public cloud platforms, and begin their journey into adoption of multi-cloud platforms, having a trusted partner to work alongside them can avoid the next set of pitfalls. Typically, integration of multi-cloud platforms into a seamless experience, having a single pane of glass for dashboard management, 24/7 monitoring and support, amongst others, are the benefits, that a trusted multi-cloud channel partner can provide for enterprises.

Rohit Bhargava, Cloud Box Technologies

"AS ENTERPRISES
SCALE THEIR
USAGE OF PUBLIC
CLOUD PLATFORMS,
AND BEGIN THEIR
JOURNEY INTO
ADOPTION OF MULTICLOUD PLATFORMS,
HAVING A TRUSTED
PARTNER TO WORK
ALONGSIDE THEM CAN
AVOID THE NEXT SET
OF PITFALLS."

Can you please elaborate on Cloud Box Technologies' new security practice? What kinds of benefits can this bring to regional customers?

RK: We recently expanded our business and launched our new security practice with team of cybersecurity specialists and an end-to-end security solutions and services portfolio. With the large-scale increase and emphasis on digital transformation in the postpandemic workplace, threat, risk, and vulnerability levels, have also increased across enterprises. With this new launch, we have adopted a holistic approach in offering our cybersecurity services, which is a business enabler for enterprises in the region that are tackling transformation technologies in the new normal.

CBT has adopted a threestep approach in expanding our cybersecurity services within our end

user customer base. These include detecting and identifying system and network vulnerabilities and risks; protecting people, processes and technologies and responding to events and incidents; and recovering data and information and monitoring cybersecurity incidents in real time.

It is essential and vital that we have this framework in place. The solutions that we design, deploy and implement at customer sites are prone to threats and can be compromised at any time. Usually end user networks are not secure and have less than the desired requirements in place. It is our responsibility to secure customer assets wherever we have deployed our solutions. That is why we have added a cybersecurity framework in our portfolio wherever we are offering technologies and solutions.

CBT's security practice is led by Rohit Bhargav, Practice Head – Cloud and Security, who has an international networking and systems engineering background of over 15 years and is experienced in enterprise networking and security having previously worked at Dimension Data, Chatsworth Products (CPI) and Huawei.

Our cybersecurity portfolio and services now include system protection, network and data protection, cloud security, identity and access governance, and managed and professional security services. To deliver these, CBT has partnered with global vendors such as Fortinet, Sophos, Pulse Secure, Digital Insights, Forcepoint, Tenable Security, Symantec, amongst others. Recently, CBT also became a Dell Platinum partner offering Dell-EMC and RSA security solutions.

What differentiates Cloud Box Technologies' security offerings to its counterparts in the market?

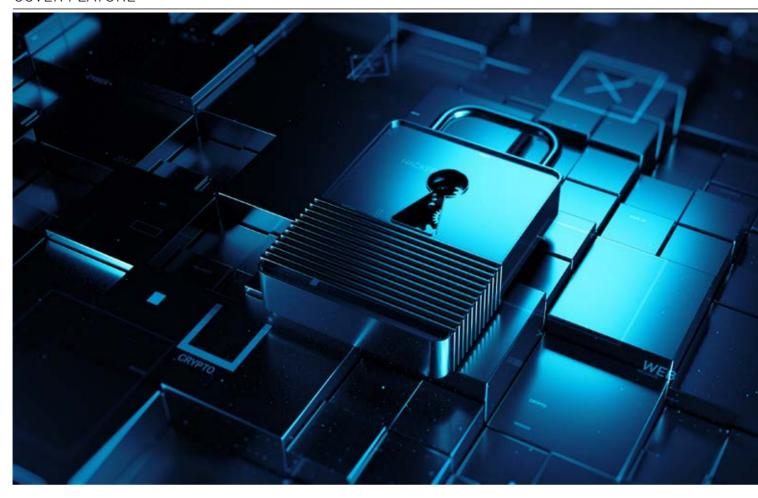
RK: Cybercriminals are operating highly sophisticated organisations with a variety of low-cost, readily available hacking tools, according to Gartner. A lack of relevant skills and low cybersecurity budgets means that organisations are falling behind in their attempts to counter the growing number of cyber-attacks. CBT is attempting to fill this gap for additional resources, to mitigate the threat of cyber-attacks, that can lead to data breaches, loss of intellectual property and regulatory exposure.

We have now embedded cybersecurity solutions into our core technology and infrastructure solutions. This ensures that no digital transformation project initiated by CBT, increases the attack surface across any of our enterprise customers and leaves them vulnerable. We protect our customers as they begin or advance along their transformation journeys, whenever we are partnering with them.

Ranjith Kaippada, Cloud Box Technologies

"WE PROTECT OUR CUSTOMERS AS THEY BEGIN OR ADVANCE ALONG THEIR TRANSFORMATION JOURNEYS, WHENEVER WE ARE PARTNERING WITH THEM."

www.tahawultech.com NOVEMBER 2020



Where do you see the enterprise cloud security space evolving in the next few months?

RB: Remote working in the current situation has given rise to a whole level of attention being paid to both cloud adoption as well as cloud security. It is important to strategise and have security priorities in place whether it is related to infrastructure, networking and applications. There are essentially two aspects that need to be tackled in cloud security, on the one hand it includes IT administration and on the

other hand it must be tackled at the users' end. We also advise enabling multi-factor authentication for both the console as well as the root user and further strengthen user authentication. With necessary permissions in place it helps reduce the attack surface by detecting users and roles.

Organisations must also check if the basic login information and configuration is correct to enable better visibility of the public cloud. And most important, adopting cloud security technologies such as Cloud

Access Security Brokers (CASB), Endpoint Detection and Response (EDR) and Cloud Data Loss Prevention (DLP) solutions for web and email, endpoints, network and mobile, most remote working workforce can be secured, centralised, managed, and threats and events can be reported and remediated in real time.

What can the market expect from Cloud Box Technologies in the coming months?

RK: Our goal is to consistently deliver exceptional cost-effective services to our customers and become the single source for all their IT and professional services requirements. We will be expanding our operations to include more countries and services as well as partnering with new global vendors who offer innovative as well as emerging technologies. 1

"WE HAVE NOW EMBEDDED CYBERSECURITY SOLUTIONS INTO OUR CORE TECHNOLOGY AND INFRASTRUCTURE SOLUTIONS."

REGISTER TODAY!



BICSI EMEA Conference & Exhibition

Virtual Online Event • 17 - 18 November 2020

Leading the Future for the Connected World





"THE IMPLEMENTATION OF A LEAST PRIVILEGE APPROACH IS ABOUT LOCKING DOWN WHAT YOU CAN AND CAN'T GET ACCESS TO, WHICH CAN ULTIMATELY HELP SECURITY TEAMS TO BETTER MITIGATE NUMEROUS VULNERABILITIES."

any sort of opportunity, they write zero-day attacks to target people working from unsecured endpoints or networks. In the past, maybe an organisation's employee takes their corporate devices to use at home or uses their personal laptops to access corporate environments, these scenarios are quite routine and security teams can address any potential issues post-haste. But if you apply that to billions of people that are now working from home, are corporate environments ready to deal with that? The answer that we've seen is – definitely not.

We've seen organisations across the world scramble to find a strategic approach to remote access, which have opened challenges for endpoint security. So, at the center of this conversation, the endpoint is where this pandemic has hit security.

How can enterprises enhance their endpoint security strategies? In addition, how can they ensure that their employees are adhering to the right security measures without stifling their productivity?

Building trust within the workforce is fundamental to any security strategy. A key approach that organisations can take to succeed in this is implementing a 'least privileged' methodology. What this means is restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform specific activities. It sounds a bit draconian but this allows organisations to control only what's required for employees to do their job roles.

The implementation of a least privilege approach is about locking down what you can and can't get access to, which can

ultimately help security teams to better mitigate numerous vulnerabilities.

At the same time, least privilege also applies to processes, applications, systems, and devices, in that each should have only those permissions required to perform an authorised activity. So, if somebody clicks on the link that's actually a phishing email and it releases a malware that laterally moves around your IT environment, having a least privilege model will enable you to control or restrict the movements that are coming from that specific system or application.

How can organisations effectively mitigate today's evolving cyber risks?

If you think about the Lockheed Martin kill chain, a cyber-attack can be broken down into seven distinct steps – reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and actions on objective.

Understanding these levels of the cyber kill chain can help you mitigate and control the security risks. It will allow you to create a useful framework for reducing cyber exposures. By applying the right layering of cybersecurity controls, organisations can get better at preventing attacks altogether, disrupting in-progress attacks, and minimising the impact of a breach should one occur.

Additionally, BeyondTrust also zeroed in on the role that privilege access management (PAM) play in mitigating modern cyber-attacks and shrinking the attack surface. We believe that Universal Privilege Management is critical in elevating PAM. This approach addresses the entire universe of privileges across

organisations, which continues to grow with the expansion of cloud, internet-connected devices, dynamic DevOps, and more. The Universal Privilege Management model offers a holistic approach to securing every privileged user, session, and endpoint, guiding organisations along a journey that allows them to address critical risk areas and immediately begin shrinking the attack surface. By implementing this approach enterprises get absolute control over every privilege in their environment.

What can the regional market expect from BeyondTrust in the coming months?

We've opened our regional office about five years ago. Since then we have grown significantly, we now have over 20 people in our Middle East office. We have sales teams, commercial teams, technical teams in Saudi and in the UAE, covering Kuwait, Oman and Bahrain as well as other markets outside the Middle East. We have the entire support platform that is unmatched in terms of the vendors that we would compete against in the market.

We also have an amazing channel ecosystem. Another strength that we have would be on trust. We were here first. So, we have the strongest channel network as compared to any of our counterparts in the market. Between us and our channel partners, we utilise each other's strengths, which puts us in an exceptionally strong position in the marketplace.

Looking ahead, you'll see a bigger investment from BeyondTrust, not only in supporting enterprise clients, but also in the corporate mid-market, where we see huge opportunities. Our products, specifically our cloud-based solutions are very apt for the requirements of remote enterprises today and we will continue to build on that. We will remain committed to helping all customers across the spectrum of the regional market to understand and achieve what true privileged management means. \$\mathbb{L}\$

www.tahawultech.com NOVEMBER 2020 19



ansomware can plague operations and hamper everything from public safety to transportation and waste management. As the GCC is embracing the rapid pace of digitisation and diversifying its economy by shifting towards digital and investing in the latest technologies, cybersecurity becomes paramount. According to a recent forecast by Gartner, MENA enterprise information security and risk management spending will total \$1.7 billion in 2020, an increase of 10.7% from 2019.

An investment in the right technology and careful execution of cyber procedures

will immediately transform the security posture of local governments and organisations. While it may not be known when a threat will come, these steps can help mitigate the effects of a breach:

Develop a cyber playbook

Like agencies that have preparedness plans to protect and respond to natural disasters, cybersecurity teams also need to plan in advance for cyber incidents, including the development of playbooks with varying scenarios.

The cyber playbook should have a comprehensive approach to security focused on identifying, protection,

detecting, responding to and recovering issues within an environment. It should also be aligned to national cybersecurity frameworks. IT leaders must ensure the playbook isn't stagnant as the organisation continues to evolve.

Train, train and train again

Security teams should always utilise opportunities for continual training. When a new member joins the team, use the onboarding process to reintroduce exercises and best practices to the whole team. Leaders should also leverage creative methods—including team events and gaming-based training,



"THE CYBER PLAYBOOK SHOULD HAVE A COMPREHENSIVE APPROACH TO SECURITY FOCUSED ON IDENTIFYING, PROTECTION, DETECTING, RESPONDING TO AND RECOVERING ISSUES WITHIN AN ENVIRONMENT."

Michel Nader, Dell Technologies

resources are undeniable.

A successful way to bridge this gap is through a hybrid managed service model, which includes a combination of civil servants and support

agreements with private sector companies that help augment resources to respond quickly in the face of cyber incidents.

such as capture the flag and software that simulates attacks—to facilitate greater participation and learning. These scenarios should include best-case and worst-case outcomes of an attack.

Awareness training is also key for teams to be able to identify and respond correctly to suspicious activity within networks.

Audit (and supplement) personnel

Cyber leaders should continually audit organisational roles to determine specific strengths and weaknesses within their teams to assess their stance on risk management.

The need for cyber talent is clear – The lack of cyber personnel and

Proper cyber hygiene

Cyber hygiene isn't a one-off exercise — It's a consistent mindset that encompasses all parts of our life and a continual journey. As governments and organisations reinvent the ways they operate and interface with constituents, they must also empower employees through a workforce transformation to meet the growing security expectations of the 21st century. This needs to be a year-round effort, with substantial, calculated investments in employees through awareness campaigns.

Cyber hygiene and culture begin at home. It's important agencies and employees educate using phishing exercises and cyber literacy, helping understand the possible negative consequences both at home and in the workplace.

Invest in infrastructure with built-in security

Agencies struggle to protect the numerous endpoints that fall outside of the traditional security reach of the organisation. As the number of tools and cloud-based systems increases, the volume of generated data also rises, expanding IT infrastructure beyond data centres, making it harder to protect against threats.

It's vital then for governments to invest in a secure, flexible infrastructure from the beginning, extending from edge to core to cloud. Doing so will allow them to focus on continually improving citizen experience without having to worry about the disruption of layering security on top.

The road ahead

An investment in a comprehensive security approach saves invaluable time and resources, and also preserves public trust. Fighting ransomware is an iterative process that measures progress. Organisations should tailor these efforts to make the most significant impact and meet with their business peers to re-assess risk and adjust the course of cybersecurity programmes accordingly.

www.tahawultech.com NOVEMBER 2020 21



oday, the success or failure of any business relies on the effectiveness of their digital transformation strategies.

The primary goal of any digital transformation initiative is the same for all organisations, whether small or large – to use technology to transform any service, process or experience into something more agile, flexible and cost-effective.

In order to realise and leverage the complete potential of digital transformation goals and technologies, organisations need to understand how cloud, cybersecurity and the channel can add genuine value and pave the way to their success.

Cloud plays a critical role in enabling organisations to achieve this objective, making it an essential first step towards digital transformation.

Over the last decade, we have witnessed cloud evolve from being an industry buzzword to a key agent for business transformation. Cloud is fueling a whole host of innovation, enabling businesses to stay relevant and thrive in today's dynamic digital ecosystem. According to an IDC study, more than 80 percent of companies are already using cloud services and cloud technology or are dealing with it intensively. By embracing the cloud, businesses can not only power innovation but also reap benefits such as a modernised IT infrastructure, enhanced collaboration and streamlined processes, allowing them to reinvent themselves to deliver exceptional value to customers.

However, to illustrate cloud as just a tool to improve traditional IT, as a

better way to maximise resources or as a method to cut costs, is to sell it far short. Organisations need to look at it with a more expansive and ambitious view. They have to realise that with the right vision, strategy, methodology and platforms, the cloud can be a catalyst for a pervasive digital transformation that will reverberate in the years to come.

In the Middle East, cloud is increasingly becoming entrenched in corporate IT strategies as digital transformation gains traction in the region. A study by global research and analyst firm IDC highlighted that digital transformation will drive cloud investments, propelling the market to reach \$2.7 billion in 2020. We have seen that many technology players including AWS, Microsoft, Alibaba, and SAP have been quick to recognise the region's



work environments and rising demands for cybersecurity are driving the need for a trusted advisor that will empower organisations to adapt and thrive.

As a global cloud and cybersecurity value-added distributor (VAD), Exclusive Networks is accelerating the market entry and growth for innovative cloud and cybersecurity technologies. We are devoted to bringing in world-class technology vendors and empowering resellers to accelerate digital transformation in the region.

Our business model of 'single-touch/ multiple markets' specialist distributor has made us the number one choice for vendors and resellers alike. Exclusive Networks has a unique market approach that combines specialist value-added technical and marketing support with the extensive reach of a global distributor, continuously redefining what it means to be a VAD.

We constantly evolve to stay ahead of fast-changing markets and technologies to stay relevant to our vendor and reseller partners. We have been very focused on building a portfolio with vendors who are best in their field and investing in our people because we believe only a highly committed team can drive business growth and success. We now have 22 vendors across our cloud and

"NOW MORE THAN
EVER, AS DIGITAL
TRANSFORMATION
CONTINUES TO REDEFINE
BUSINESSES, THE CHANNEL
NEEDS TO BE IN SYNC AND
ENABLE CUSTOMERS TO
NAVIGATE THE COMPLEX
TECHNOLOGY LANDSCAPE."

cybersecurity portfolios – including recently onboarded partners Vectra, Checkmarx, Quest, One Identity and Hycu – all of which deliver unique market capabilities and technologies.

Subsequently, reseller partners around the world rely on us to create new business opportunities and generate revenue streams from new technologies. We also continue to demonstrate our unwavering commitment to empowering our partners by continuously delivering innovative enablement initiatives through our regular cloud and cybersecurity workshops; our Cloud Training Centre, which offers authorised and approved cloud training to technical and sales teams across the region; and our Cyber and Cloud super centre, which has gone from strength to strength since its launch two years ago.

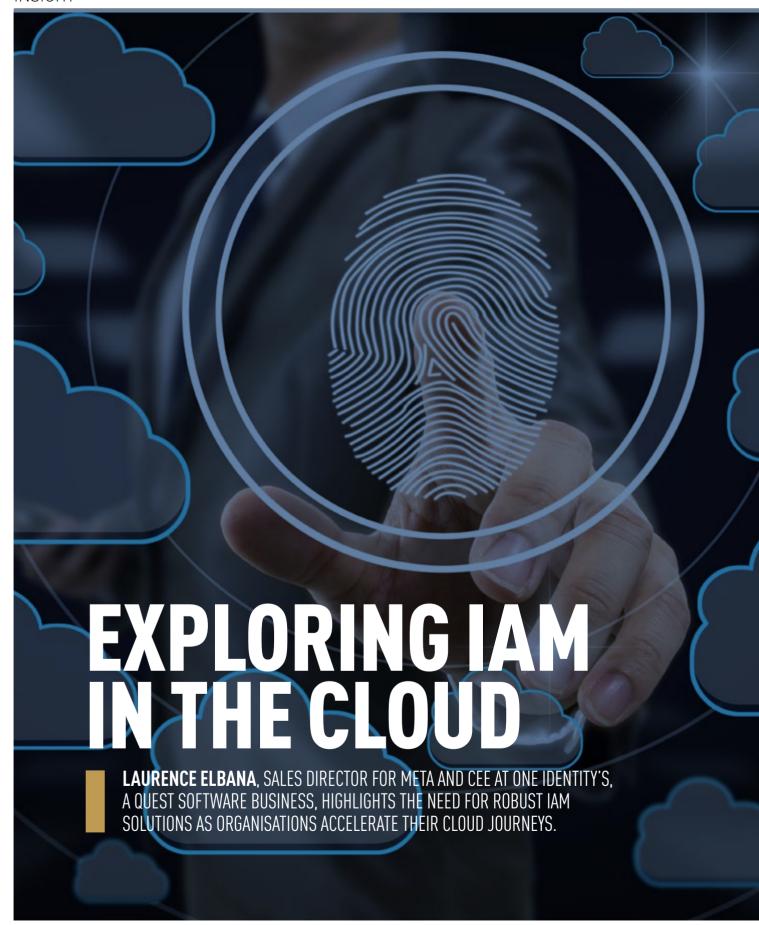
In a day and age where digital is king, organisations need the right foundations to emerge successful. This means getting cloud and cybersecurity right from the onset of their digital transformation journey is paramount and leveraging an expansive ecosystem is advantageous. As a trusted specialised cloud and cybersecurity VAD, we are constantly evolving and improving our capabilities to enable customers and partners alike to make great strides in the digital era. 1

cloud-readiness and have begun investing in Middle East-based cloud data centres.

While digital transformation presents boundless opportunities, it is not without its challenges. The shift to digital results in interconnected systems and increased number of endpoints, which could leave organisations vulnerable to cyber risks and threats. This highlights the vital role of cybersecurity in digital transformation. Business leaders today are realizing that they can no longer afford to make cybersecurity an afterthought and are considering it as a key investment priority next to the cloud.

Now more than ever, as digital transformation continues to redefine businesses, the channel needs to be in sync and enable customers to navigate the complex technology landscape. Increased cloud dependence, fragmented

www.tahawultech.com NOVEMBER 2020 23





"ENTERPRISES TRADITIONALLY
USED ON-PREMISES IAM SOFTWARE
TO MANAGE ACCESS TO MULTIPLE
RESOURCES. BUT AS COMPANIES
ADD MORE CLOUD SERVICES TO THEIR
ENVIRONMENTS, MANAGING SUCH
ACCESS IS BECOMING MORE COMPLEX."

s customers move to the cloud, they are faced with immediate requirements of managing users on-premise as well as in the cloud. Cloud deployments often result in having to deal with multi-tenancy and third-party managed infrastructure, which necessitates a strong identity and access management (IAM) strategy.

IAM solutions need to be built on a clear identity strategy and policy within an organization. All the identity, access and management solutions must be centralized on a platform that will not only enable customers to create users but also manage them and be able to produce the reports that can be shared with auditors and compliance teams. This way organizations gain visibility on what users are doing and who has access to what accounts and systems. It also ensures all users are compliant and no one is above the policies set by the business.

Enterprises traditionally used onpremises IAM software to manage access to multiple resources. But as companies add more cloud services to their environments, managing such access is becoming more complex.

To address this complexity, One Identity provides customers with the tools to synchronize both environments and create

central management solutions. We have use cases for all strategies with our on-premise, cloud and hybrid identity management solutions. This way we can cater to a specific customer's environment, be it completely cloud or on-premise or a hybrid one.

Another primary use case for One Identity is the Identity Lifecycle Management, often called provisioning or joiner/mover/leaver. It is essentially the journey employees make in their roles within an organization when they join. Our offerings allow IT and security teams to accurately enable and provision for accounts for those users – for example, Office 365 and cloud accounts, Salesforce Cloud System and so on.

Boasting an end-to-end IAM portfolio, One Identity plays an effective role in helping customers address identity and access management challenges. We are continuously eliminating identity challenges and help secure enterprises seamlessly as they accelerate their digital transformation journeys.

One Identity's pioneering solutions complement Exclusive Networks' security portfolio perfectly. As our go-to-market distributor partner, we will work hand in hand with Exclusive Networks to cater to the increasing customer demands for identity access and management solutions in the region.

www.tahawultech.com NOVEMBER 2020 25

MODERNISING DIGITAL WORKPLACES



highlights at Quest over the past year.

Quest Software has been catering to customers'

IT management and security requirements for over 30 years. In the past 12 months, we have evaluated our portfolio that houses over 125 products and reorganised our technology into three main pillars – manage, modernise and secure.

lease share some of the

The modernise pillar of Quest, which is around modernising workplaces and ideal workloads, has been a pivotal focus over the past year as we've seen a huge shift in the market towards this goal. We have also acquired a couple of the prominent players in the market – Binary Tree, ApexSQL and Metalogics. These two milestone acquisitions have been our biggest highlight over the past year.

How has the increased adoption of a multi-cloud approach changed demands around data management and protection solutions?

Over the recent months, we have witnessed organisations fast-track their cloud journeys. This shift in the market has greatly driven the demand for data management and security solutions.

As part of this changing market

dynamics, Quest is helping customers modernise their IT by shifting to the cloud. We have added more technologies into our portfolio that would enable us to seamlessly move workloads such as email, file share, SharePoint and so on, to the cloud without any operational disruptions to customers.

How can Quest solutions enable the effective governance of modern cloud deployments?

What makes Quest solutions exceptional and stand out in the market is the fact that we not only have the expertise to move workloads but also have the technologies to run them in the cloud. Our offerings provide easy access, ensure the data is audited appropriately and are compliant with the enterprise's internal policies as well as local and global regulations.

What can regional partners and customers expect from Quest in the coming months?

Over the next four months, we will be releasing Partner Circle 2.0. Our channel community can expect even bigger rebates, more margins and increased profits from the new program. The market will also see us acquiring more companies around cloud workloads towards the end of the year.

What role will Exclusive Networks play in your upcoming initiatives?

Exclusive Networks is a critical partner for us as our dedicated value-added cloud and security distributor for the region.

We've been working together for about a year, and jointly we've been able to develop the Saudi, UAE and Egypt markets. They have given us access to extensive reseller networks and end-users.

NORDEN®

Reliable fast connection for all...



Dielectric Self-supporting figure 8-Aerial cable from Norden ensures protection from UV rays and other harsh environment factors. The lightweight wires also offer a good bend resistant performance making it more durable and reliable. The cables are made of standard galvanized steel and are designed for medium span aerial installations. They have ultraviolet and harsh external environment protection. Up to 12 fibres are there in each jelly filled plastic compound tube, which are stranded around a FRP strength member, water blocking tape and covered by a PE outer sheath. The upper part of figure 8 has seven number messenger wires made of stranded galvanized steel wire with PE outer sheath. They have small diameter, light weight, good bend resistance performance. The messenger cables support the fibre cables to withstand the tensile force for aerial installations. The PE outer sheath gives excellent environment and ultraviolet protection to the cable.



READY AND SECURE

RAQMIYAT DIRECTOR FOR CYBERSECURITY AND INFRASTRUCTURE **ABHIJIT MAHADIK** SHARES VALUABLE INSIGHTS INTO HOW SECURITY PRIORITIES HAVE SHIFTED DUE TO THE COVID-19 PANDEMIC AND HOW ORGANISATIONS CAN STAY SECURE AND COMPETITIVE IN THE NEW NORMAL.

he ongoing COVID-19
pandemic has significantly
transformed the way
businesses operate today.
How has this shift impacted
security investments and strategies?

Post-COVID, we are seeing a major change in the way business is done. The new normal way of doing business is emerging, changing the entire cybersecurity threat landscape. Threats are also evolving as is the new normal in parallel. Investment priorities have also shifted as per the new normal. We believe CISOs and cybersecurity teams will continue to make various security niches high priorities for spending including perimeter security, as customers will continue to prioritise short-term spending on security for remote workers. Secondly, they will increase their focus on next-generation identity and access controls. Customers that had delayed adding MFA to legacy systems are now accelerating its adoption or are moving to cloud platforms.

As expected we will also see amplified

investments on solutions around remote access as CISOs continue to support virtual workarounds for help-desk staff who would work in the office under normal circumstances. Finally, we expect that the cyber awareness training—that developed in-house and that delivered by an outside provider—that CISOs offer will be adapted both to cover remote-work situations and bring-your-own-device policies and to be delivered virtually.

How can IT and business leaders implement robust security measures while ensuring that their employees are in tune with such procedures without stifling productivity?

Before deciding to enforce work-fromhome policies, businesses, IT and security teams need to conscientiously assess their resources. They also need to project how much the implementation will strain the IT team and assess what risks must be factored in and address.

Organisations need to also consider deploying security solutions that feature strong web security protection on

employee endpoints, as well as technologies capable of preventing network vulnerabilities from exploitation. Another key aspect that they need to keep in mind is setting up and supporting a conferencing software that ensures a stable voice and video connection, as most meetings will occur virtually and reliability is key. Furthermore, employees may need reminders to ensure that they adhere to proper cyber hygiene such as changing their passwords before leaving the office, therefore, sending out rules and guidelines to ensure that employees are in tune with such procedures without stifling productivity.

What solutions or technologies should organisations focus on to ensure that their security measures are future-proof?

We have been seeing CXOs struggling to cope with rapidly changing areas such as endpoint security and privacy, access control and governance as well as unified cybersecurity compliance and automation, as they continuously adapt

"RAQMIYAT PLAYS A
VITAL ROLE IN ASSISTING
CUSTOMERS IN THEIR
EVOLVING CYBERSECURITY
NEEDS BY PROVIDING
THEM WITH THE RIGHT
CONSULTANCY, SERVICES
AND ROADMAP FOR A
SECURE FUTURE."

to remote working or hybrid working models. Organisations should adopt and focus on these areas to ensure that their security measures are future-proof.

A major challenge for enterprises has been maintaining business continuity while ensuring cybersecurity. As a key player in the regional IT and security industry, how is Raqmiyat enabling organisations to stay secure while remaining agile amid the 'new normal'?

The COVID-19 pandemic has made a significant impact on cybersecurity. Simply put, for customers, it required them to invest more time, efforts and resources to maintain their security postures. Subsequently, it also placed greater responsibilities service providers in terms of effectively supporting organisations and their security needs. Ragmiyat plays a vital role in assisting customers in their evolving cybersecurity needs by providing them with the right consultancy, services and roadmap for a secure future. Post-COVID, Ragmiyat aims to further support customers and businesses who are struggling to keep up with doing business in the 'new

Where do you see the security landscape heading in the next few years, what best practices should organisations adopt to cope in a post-COVID-19 world and stay competitive?

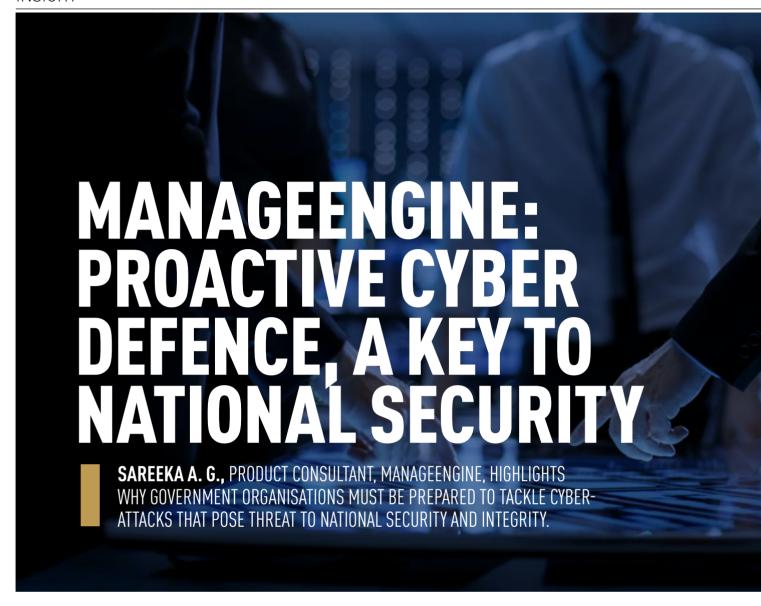
With the outbreak of COVID-19, there are widespread extended requirements for staff to work from home. The phrase 'work-from-home' brings-in fears on data security. It also increases the security risks brought by unmanaged

endpoints such as end-user owned remote desktops, PCs and laptops used by staff, external vendors, partners and contractors.

CXOs are worried regarding security of sensitive corporate information, as their workforces are now spread geographically and are operating out of uncontrolled, unsecured home environments. Therefore, securing these unmanaged devices will be key to staying resilient and competitive. Tools such as threat monitoring solutions based on dynamic and agile threat models will also play an important role in the future.

normal', new advanced technologies and digital transformation and the evolving cybersecurity threat landscape.

www.tahawultech.com NOVEMBER 2020 **2**



igitisation and advancements in information and communication technology have revolutionised every aspect of modern life. While a connected digital ecosystem that intertwines critical infrastructure provides enormous potential for innovation and development, it also increases the attack surface. The way a country responds to the opportunities and risks that arise in cyberspace plays a crucial role in its growth and security.

Though we all acknowledge the imminent risks cyber attacks pose, are we aware of the scale of impact such attacks can have on a country and its

people? Let's explore the impact as well as who the attackers are, and how they can be stopped.

Who are the attackers and what can they do to a nation?

Based on their motives and scale of attack, cyber attackers can be classified into four groups:

• State sponsored attackers are nonstate individuals or organisations who are discreetly supported by a government entity. These attackers generally operate to fulfill political, commercial or military interests of their country of origin. In today's world of mutual distrust where nations want to have an upper hand over others, state sponsored cyberattacks have become commonplace. Attackers use a combination of different techniques ranging from spear phishing attempts backed by well-researched social engineering to sophisticated advanced persistent threat (APT) campaigns in order to infiltrate networks and gain access to confidential information such as trade-secrets, research findings, and war strategies to name a few. Cyber espionage and insider attacks (where a trusted insider is paid for carrying out parts of the attack) are also not uncommon. State sponsored attacks have the potential to crumple



"IN TODAY'S WORLD OF MUTUAL
DISTRUST WHERE NATIONS WANT TO
HAVE AN UPPER HAND OVER OTHERS,
STATE SPONSORED CYBER-ATTACKS
HAVE BECOME COMMONPLACE."

appears to be just a form of electronic civil disobedience without malicious intent, taking down networks of organisations that provide essential services such as hospitals can have devastating impact on citizens' lives.

hacktivism

 Organised criminal networks are groups of malicious individuals who form centralised enterprises to carry out illegal activities for profits. Some of the criminal organisations have a political agenda and carry out attacks to induce terror.

Supervisory control and data acquisition (SCADA) system communication networks form the backbone of industries such as electricity distribution, aviation, manufacturing, waste and water control, oil and gas transportation, and others that are crucial components of a modern economy. The SCADA systems are employed to manage physical processes and sensitive functions. Attackers can compromise the communication networks either by gaining direct physical access to the plants or by establishing remote access. Once the attackers have control over the SCADA systems, they can manipulate crucial controls and cause physical harm or gather intel to use in an actual terror strike that creates a devastating impact.

 Low-level individual criminals are hackers who compromise individual devices or organisational networks for monetary or personal gains. They usually launch small-scale attacks and do not have any hidden agenda.

This type of attacker might seem to be an implausible threat when you think of national security. But let's not forget that national security doesn't just involve protecting the borders, it also includes securing a nation from within.

Amid the COVID-19 pandemic, governments across the world are employing initiatives and leveraging technology to contain and cure the disease. Imagine this scenario: You receive an SMS allegedly from the Ministry of Health, advising you to download a mobile application that will warn you when a COVID-19 affected person is in your vicinity. Sounds like a wonderful way to keep yourself from getting infected, doesn't it?

The problem is, the SMS could actually be a phishing message, and the app could

entire nation-states when the right data is compromised.

 Hacktivists are individuals or groups of individuals who use cyber-attacks as a way of expressing political or ideological extremism.

Numerous cyber-attacks have been carried out in the past as a means of expressing resistance. Launching large scale distributed denial of service (DDoS) attacks to render government servers inaccessible and loading videos and images that criticise a state's policies on government websites are some of the most common methods hacktivists employ to make their voice heard. While

www.tahawultech.com NOVEMBER 2020 **3**°

be malicious and gather information from your mobile device. This information may then be relayed to attackers who can demand a ransom, take control of your device, and commit identity fraud and other crimes. Such an attack on a small scale might appear insignificant, but when thousands of unaware individuals fall prey and their identities are misused, it can lead to a massive security crisis.

Combating cyber threats

Cyber threats have become a continually evolving and complex security challenge. Implementing a complete, all-inclusive approach towards improving IT security in both physical and virtual realms is the need of the hour.

Fortify physical security

Government and private organisations that house sensitive information must protect their premises from physical attacks by carefully scrutinising and permitting entry only to authorised individuals. A combination of identifiers such as pass codes, ID cards, and biometrics should be employed. Around the clock surveillance as well as proper maintenance and physical isolation of sensitive servers and devices are essential to prevent attackers from gaining manual access to the facilities and tampering.

Locate and fix vulnerabilities

Conducting risk assessment is one of the first steps towards creating a secure IT environment. List all the data assets, identify associated vulnerabilities and the likelihood of being compromised, and estimate the magnitude of impact. Using this information, classify each data asset as a high-, medium-, or low-risk entity and apply appropriate protection controls. Once assets have been classified, scout the network for vulnerabilities and fix them. Continuously tracking all security information and events is essential to monitor the health of an organisation's IT network. Virtual private networks (VPNs) and multi-factor authentication (MFA) techniques can be used to secure connections over unreliable networks and to prevent credential misuse, respectively. Having up-to-date systems and applying timely software patches can also help protect network devices.

Prevent insider attacks

While perimeter defense mechanisms such as firewalls and proxy servers can help prevent intruders, tackling insider attacks requires a different strategy. Insiders already possess the permissions required to access critical assets that they want to compromise. An adversarial nation-state could compromise an insider's credentials or incentivise a trusted employee to work for it. With the help machine learning (ML) and artificial intelligence (AI) technologies, baseline behaviour can be established for all the user accounts and entities in a network. By comparing the current activities of a user or entity with the baseline behaviour. suspicious activities can be detected and IT admins can be alerted.

Automate threat response

Advanced SIEM tools can be customised to perform automated threat response functions such as suspending malicious accounts or temporarily denying permission to perform certain activities. In case of an attack, this enables IT administrators to limit damage, protect surviving assets, and help in business continuity. Modern cybersecurity tools have the capability to correlate vast event

"CONDUCTING RISK
ASSESSMENT IS
ONE OF THE FIRST
STEPS TOWARDS
CREATING A SECURE IT
ENVIRONMENT."

logs, deduce imminent cyber-attacks, and warn security experts. These tools also generate extensive reports that aid in forensic analysis of a cyber-attack.

Regulate cybersecurity

Apart from the possible ways to prevent cyber-attacks from an IT security standpoint discussed above, protecting cyberspace requires the formulation and efficient deployment of strict cyber laws and regulations. Well-defined rules that explicitly describe criminal activities and associated penalties and punishments will provide a systematic and legal approach to deal with cyber-attacks and attackers.

Just like the geographic or physical boundaries, a country's cyberspace requires constant surveillance and security. As a first step to getting started, governments should acknowledge the danger that cybercrimes can pose to a society and act accordingly. Ensuring cyber safety is a combined effort. Without active participation of individuals, cyber laws would just be statements on paper. Coordinating a multi-agency response and executing preventive and counteractive measures against cyber threats in judicious proportions is the way ahead. \$\mathbb{1}\$



6-10 20
DEC 20
DUBAI WORLD TRADE CENTRE





Be part of the year's only global tech event, LIVE in Dubai

Co-located with



FUTURE BLOCKCHAIN SUMMIT قمة مستقبل البلوك تشين



GITEX.COM

#GITEX2020

Some of our 2020 Exhibitors

























Derek Manky, FortiGuard Labs

Aamir Lakhani, FortiGuard Labs

A SNAPSHOT OF THE CURRENT THREAT LANDSCAPE

DEREK MANKY (DM), CHIEF, SECURITY INSIGHTS & GLOBAL THREAT ALLIANCES AND **AAMIR LAKHANI (AL)**, GLOBAL SECURITY STRATEGIST AND LEAD RESEARCHER, FORTIGUARD LABS, PROVIDE SOME INSIGHT INTO THE MINDS OF CYBERCRIMINALS AND THEIR VARIOUS TACTICS AND TARGETS.

hat changes in attack
trends has FortiGuard
Labs seen in the months
since the beginning of
the pandemic?

DM: April and May were the months where the most COVID lures came about, and of these, email-based threats were by far the most dominant in the threat space. These threats played off of layoff notices sent to employees, false purchasing orders, messages from HR departments, really anything that could exploit the huge shift in the work environment that employees were experiencing. Outside of the workplace, people were being targeted by health authority impersonators for example offering more information about the pandemic. In our trackers, the traditional COVID lures have dropped down quite a bit, going from almost 350 a day to double digits now. Now that things are shifting to a different normal, we're seeing the old threats kickoff once again, but with a change

Derek Manky, FortiGuard Labs

"I BELIEVE THE NEXT 2-3 MONTHS IN CYBERSECURITY WILL BE QUITE CRITICAL AND IT'S REALLY THE TIME TO SET UP A STRONG FOUNDATION BUILT ON ACTIONABLE THREAT INTELLIGENCE."

in general focus. For example, as some organisations begin hiring again, we're seeing lures that are specifically targeting candidates, particularly with man-in-the-middle attacks. For example, bad actors are injecting themselves into the middle with classic threat attempts such as sending malicious PDFs as resumes.

The attack surface for threat actors is constantly growing, are there any targets that stand out to you as most vulnerable?

DM: Cybercriminals are often going to jump on the freshest opportunity they see for the element of surprise but that varies from place to place. The start of Q4 means a lot of people are heading back to work, but also students are heading back to school—both remotely and in-person, or a combination of the two. And that's been a huge challenge for some institutions that weren't fully prepared with remote learning capabilities, particularly in K-12 learning where this is all very new to them. They have new platforms and classroom setups, as well as a lot more connections that are happening, so education is a big target right now.

AL: Attackers have also shifted their focus to areas where people are becoming more digitally populated. Things like remote learning are still ongoing in places like the U.S., so we're seeing more service and online attacks aiming to disrupt these organisations. It's almost the perfect situation for attackers because a lot of schools are set up with a hybrid learning model, where teachers are headed to classrooms while doing remote work and teaching. All attackers have to do is target the

internet connections being used in the classrooms, rather than targeting cloud applications or other platforms. By doing this, these bad actors can target more institutions and users much quicker.

What are some of the most popluar attack vectors right now?

DM: There are a lot of systems that are now publicly exposed, especially with increased usage of Remote Desktop Protocol (RDP). Attacks like Wannacry, for example, leveraged public RDPs as points of entry and we know that was a big concern. This is something that I think, from a security architectural standpoint, needs to be addressed still. When it comes to remote learning especially, it's such an easy way for attackers that are trying to hijack these sessions to try to get into these networks.

AL: Last year, I remember doing a search on Shodan to see how many publicly available RDP ports were indexed and the number then was a little over 2 million. I searched again a few days ago and it was over 4 million worldwide. We've definitely seen an increase in public RDP connections out there, which means this is a growing risk. At this point, most RDP connections are on the public network and it's an easy win for attackers.

What would you recommend defenders do given what we know about the threat landscape in 2020?

DM: This is where our world of threat intelligence really comes into play. We often say you can only protect against what you can see and I think, in the past, a lot of these attacks were not seen.

There was a lot of persistence and stealth in these attacks. Companies didn't have the proper inspections or management in place for all of their traffic flow, similar to the RDP case. Another key to defending against cybercriminals is getting the right model for securing, segmenting and monitoring business-critical applications. I believe the next 2-3 months in cybersecurity will be quite critical and it's really the time to set up a strong foundation built on actionable threat intelligence. This is the new normal we're heading into and it's important to have a structured security plan.

AL: Visibility is a key, especially these days when most traffic is encrypted. If you put in a regular firewall or other devices that are not capable of that filtration at high speed, you may miss critical threats entering your network. You need a setup that is capable of decryption and encryption as well as having the proper policies and inspections in place to sort them. Timely information is also important because you need to know the second the attack has happened and be prepared to address it, rather than finding out months after the attack actually happened.

With the rapidly changing threat landscape, do you have any predictions on where the cybersecurity conversation will be in the next few months?

DM: In the future, I think we will see more discussion around critical areas like healthcare and education, but also around operational technology (OT) as we move into more integrations. The wide adoption of technology to facilitate OT by combining old and new technology will lead to a collision between old, sometimes vulnerable technology with new technology capable of combatting modern threats. The entire ecosystem of OT is becoming a larger attack space that is often challenged with threat visibility, and this needs to be top of mind for these organisations.

www.tahawultech.com NOVEMBER 2020 35



he threat landscape continues to evolve as digitisation increases. In an attempt to keep pace, organisations are adding new software to their tech stack, but are they choosing the right solutions and approach to ensure their security? When it comes to social and digital platforms, such as social media, online marketplaces, and recruiting sites, security teams can default to treating security threats reactively rather than proactively.

Enlightened organisations are turning to Digital Risk Protection (DRP) programmes as a proactive security solution to protect their brand credibility, customers and employee safety online.

An effective DRP programme enables an organisation to respond quickly to digital threats by taking down fraudulent websites, ads and social media accounts, notifying review sites and online forums about false and misleading postings and alerting online marketplaces and app stores to counterfeit merchandise and fake mobile apps. It should also provide IT groups with current threat intelligence to limit damage from data breaches by deactivating compromised user accounts, revoking stolen credentials, and strengthening security controls.

Here are three reasons why implementing the right DRP solution and approach is a critical piece of any organisation's security defence:

Encompass the breadth of social and digital platforms

Security groups have extensive investments in staff and programmes

for detecting Indicators of Compromise (IOCs) on their network and systems, but what happens when an attacker targets their organisation's Twitter page, LinkedIn or Facebook profile, Amazon marketplace listings, or ZipRecruiter page?

Most organisations have a technology stack that is enriched with cloud-based, external-facing applications. When malicious activity, like account hijacking, impersonations, and targeted phishing attacks occurs, it is subjected to public scrutiny. Thus, compromising a brand's reputation and damaging trust. If an organisation hasn't invested resources in an effective DRP programme to monitor for fraudulent or suspicious activity, they're ripe for the picking.

A holistic DRP programme will not just cover an organisation's Facebook



page or eBay store, but will instead offer security teams omnichannel visibility into the breadth of social and digital platforms comprising that organisation's attack surface. This can include coverage of social media platforms, fraudulent domains, employee credentials on the dark web, counterfeit products being sold on Amazon and more. The expansive coverage a reputable DRP programme offers combined with automation lifts the weight off of security teams' shoulders to manually monitor threats entering their organisation's digital footprint or manage multiple different technologies for different channels.

Analyse threats within the complete digital footprint

Digital risk protection is not only about where to look, but also what to look for. Security teams need to investigate beyond the channels their

organisation owns by:

- Finding all external references to their brands, products and employees.
 - Determining where the references came from.
 - Researching if the references are legitimate or signs of malicious activity.

These three steps may appear simple, but without the right solution, it's impossible to examine all activity that treads into an organisation's digital footprint.

DRP platforms provide tools to

"DRP PROGRAMMES ARE MORE THAN JUST A
DETECTION AND ANALYSIS TOOL; THEY'RE BUILT WITH
ADVANCED ARTIFICIAL INTELLIGENCE AND SYNC VIA
API INTEGRATIONS WITH HOSTS AND NETWORKS
TO IMMEDIATELY TAKE DOWN CREDIBLE THREATS."

discover and assess references to names, brands, accounts, sites, products, executives, and employees associated with an organisation. There are several ways malicious activity can permeate an organisation's digital footprint — the table below lists a few.

Remediate and take down attacker infrastructure

DRP programmes are more than just a detection and analysis tool; they're built with advanced artificial intelligence and sync via API integrations with hosts and networks to immediately take down credible threats. The true value of a DRP solution lies in the ability to stop an account hijacker in their tracks or shut down fraudulent behaviour the second it appears within an organisation's digital footprint — before lasting damage is done.

Like all products on the market, not all DRP programmes are the same.

Consider the degree to which a DRP platform can streamline remediation and takedown activities by sending alert details and contextual information to SOC teams and analysts for rapid response and by facilitating automated takedown steps that are sent immediately to social network platforms and web site hosts.

The true value of a DRP programmeme: Brand and employee safety

Security teams are responsible to maintain security for network systems and software solutions, but if an attack occurs on a public-facing channel, employees and followers can fall victim to the scam — leading to a decline in public trust.

Security teams must expand their scope and address this ever-increasing risk.

The right DRP programme will identify threats infiltrating an organisation's digital footprint, analyse their credibility, and take action to remediate malicious activity before it impacts the organisation's reputation.

www.tahawultech.com NOVEMBER 2020 37

3 STEPS TO BOOST SECURITY FOR THE HYBRID BUSINESS



RICK VANOVER, SENIOR DIRECTOR OF PRODUCT STRATEGY, VEEAM, SHARES TOP TIPS IN SECURING A HYBRID WORKFORCE.

usinesses across the Middle
East are moving towards a
hybrid working model – with
some employees beginning
to return to offices but a
significant proportion still working
remotely in some capacity.

As sectors enter a period of recovery – and with non-essential investment set to fall – CIOs will be forced to prioritise their IT spending accordingly.

Cybersecurity poses a constant threat to businesses. This is particularly true now that so much hardware, software and data sit outside the traditional four walls of the data centre.

Outlined below are three immediate steps to boost the cybersecurity wellness of your organisation:

Shrink your shadow IT: Employees are working remotely at a scale most companies have never seen before. Whether it's because companies do not have the systems to fully support a virtual workforce, or employees have turned to consumer apps for professional use, shadow IT has grown exponentially.

To reclaim control of data sat outside their four walls, IT teams must ensure employees are aware of the best practice in terms of connecting and saving files via company-provided services or the Virtual Private Network (VPN). Furthermore, company-secured and password-protected cloud environments must be made compulsory for saving corporate files and personal cloud accounts strongly discouraged.

Manage your devices: Connected to the extension of shadow IT is the fact that

"TO RECLAIM CONTROL OF DATA SAT OUTSIDE THEIR FOUR WALLS, IT TEAMS MUST ENSURE EMPLOYEES ARE AWARE OF THE BEST PRACTICE IN TERMS OF CONNECTING AND SAVING FILES VIA COMPANY-PROVIDED SERVICES OR VPN." employees outside the four walls may be using personal devices for corporate use. For any business mandating an extended work from home policy, secure devices must be issued to prevent employees from storing potentially sensitive data on unprotected devices. Furthermore, while a password refresh is one way to up-level security overnight, embracing two-factor authentication across corporate devices is a great way to make your organisation less attractive to cyber-attackers.

Back up and protect it: This is the simplest cybersecurity rule of them all. If it's not backed up, it's not protected. Data sat outside the organisation cannot be backed up. Therefore, it's not recoverable in the event of an outage of cyber-attack. By shrinking shadow IT, organisations can increase the amount of data they are able to protect. Furthermore, organisations must ensure data within the four walls is backed up. This includes across cloudbased apps such as Microsoft Office365 and OneDrive, which do not automatically backup data, meaning it may still be unprotected.



Solviions that matter.

CloudBox Technologies is your trusted solution partner for your cloud, cybersecurity and data center solutions.

- IT Infrastructure
- Data Management (Data Backup, File / Email Archiving, Data Availability & Data Insight)
- Information Securities & Virtualization Software & Hardware Solutions deployment and Support.

WE do IT right!

Talk to us today.

Cloud Box Technologies LLC

Latifa Towers, Sheikh Zayed Road, Dubai, UAE.

Tel: +971 4 344 5022

Email: info@cbt.ae | Visit: www.cbt.ae



Modernizes your approach to secure access

RSA SecurID Suite enables organizations of all sizes to mitigate identity risk and maintain compliance without impeding user productivity. It ensures users have appropriate access and confirms they are who they say they are with a modern, convenient user experience. In addition, RSA SecurID Suite provides unified visibility and control across organizations' many islands of identity.