

Security

ADVISOR

MIDDLE EAST



PREVIEW:
GITEX 2020

ROADMAP TO CLOUD SUCCESS

HOW SANS INSTITUTE IS
DEVELOPING STRONG SECURITY
TALENTS AND ADDRESSING THE
CLOUD SKILLS GAP

+
EXPERT'S CORNER:
CYBEREASON'S SAM CURRY

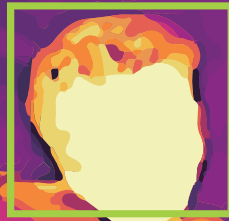
+
INTERVIEW:
KAPALYA'S MOHAMED MENAKBI

+
CYBERSECURITY 2021:
THE NEW YEAR WILL
BRING NEW CHALLENGES

FRANK KIM,
FELLOW
INSTRUCTOR,
SANS INSTITUTE



36.5° C



Hikvision Temperature Screening Thermal Solutions

SAFER, FASTER, SMARTER



Contact-free



Multi-person detection



1s measurement



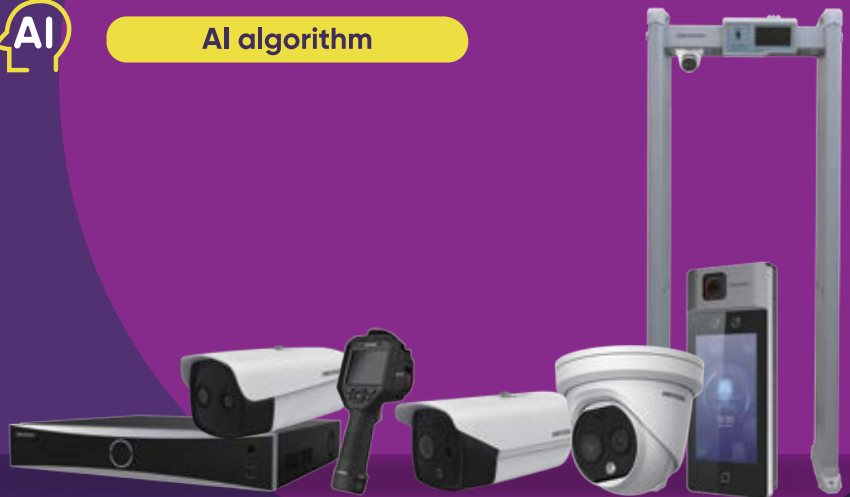
AI algorithm

Thermographic
Cameras

MinMoe Terminals

Metal Detector Door

DeepinMind NVRs



Temperature Screening
Thermal Cameras

For more information, please scan the QR-Code to visit
our Temperature Screening Thermal Solution page.

HIKVISION

www.hikvision.com

CONTENTS



10 Roadmap to cloud success

How SANS Institute's latest curriculum can enable enterprises to future-proof their cloud strategies



20



22



36

6 GITEX 2020
A preview of some of the biggest tech players participating at GITEX Technology Week

38 CYBERSECURITY 2021
Citrix spotlights the security challenges that organisations will face in the New Year

30 ACCELERATING DX POST-COVID-19
Huawei on how cloud and AI will enable enterprises to succeed in a post-epidemic era

46 LAST TAKE
Fortinet highlights the key benefits of secure SD-WAN for enterprise customers



6-10 **20**
DEC 20
DUBAI WORLD TRADE CENTRE



INSPIRING THE NEXT DECADE OF BREAKTHROUGHS

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

Co-located with



FUTURE
BLOCKCHAIN
SUMMIT
قمة مستقبل البلوك تشين

ماركتنغ مينيا
Marketing
Mania

#GITEX2020
GITEX.COM

Some of our 2020 Exhibitors



هيئة الطرق والمواصلات
ROADS & TRANSPORT AUTHORITY



EDITORIAL



Talk to us:

E-mail:

adelle.geronimo@cpimediagroup.com

Adelle Geronimo
Editor

LOOKING UP!

2020 has brought a lot of challenges to people all over the world. No one could have predicted the chaos it would bring. However that being said, it's heartening to see that many have shown optimism and resilience, and have evolved to cope and thrive despite the tough times.

While the year is coming to an end, the fight against COVID-19 is far from over. However, what we can expect is that people and businesses alike will continue to move forward, constantly finding new ways to offset the obstacles. In the technology and business world, IT and security leaders are showing their unwavering commitment to develop innovations that will ensure that their organisations can withstand today's challenges. This has been particularly demonstrated by the achievements and initiatives that were led by this year's CISO50 and Future Security Awards winners. Turn to p.22 to see the amazing individuals and organisations that

have exhibited excellence and leadership in security innovation.

Furthermore, technology events are coming back, starting with the world-renowned GITEX Technology Week, which will be the only major live, in-person tech show in 2020. For years GITEX has been the perfect platform for showcasing the diverse and ground-breaking technologies.

It clearly demonstrates that, while the year may be ending, the work that IT and security leaders have is not as they constantly innovate to take on the challenges ahead.

On that note, with great deal of optimism and gratitude, I have to reveal that this editorial will be my last. As I part from Security Advisor ME I want to say thank you. Thank you to the amazing team at CPI Media Group and to the IT and security leaders for trusting us with your stories. I trust our paths will cross again.

I am extremely proud to have been a part of this magazine and I wish it continued success! Here's to positive new beginnings!

"WHILE THE YEAR MAY BE ENDING, THE WORK THAT IT AND SECURITY LEADERS HAVE IS NOT..."

EVENTS



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

Published by

CPI MEDIA GROUP
CPIMEDIAGROUP.COM

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

Anita Joseph
anita.joseph@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Jefferson de Joya

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.

GITEX TECHNOLOGY WEEK 2020

TAKING PLACE FROM 6TH TO 10TH DECEMBER, GITEX TECHNOLOGY WEEK IS THE WORLD'S ONLY MAJOR LIVE, IN-PERSON TECHNOLOGY EVENT OF THE YEAR. AS WITH PREVIOUS EDITIONS, GITEX 2020 WILL SPOTLIGHT GROUNDBREAKING PRE- AND POST-PANDEMIC TECHNOLOGIES AND THE PIONEERS BEHIND THEM. HERE'S A PREVIEW OF SOME OF THE BIGGEST PLAYERS THAT WILL BE PRESENT AT THE SHOW.



Huawei is collaborating with partners from around the world to showcase how governments and organisations in the Middle East can create new value through synergy across five tech domains.

As this year's 5G Innovation Partner, Huawei has strengthened its commitment

HUAWEI TO HIGHLIGHT FIVE KEY TECH TRENDS IN THE ICT SPACE

CHARLES YANG, HUAWEI MIDDLE EAST

to the region's technology ecosystem by confirming its largest ever GITEX Technology Week presence at the 40th anniversary edition of the event.

As 5G has been rolled out at scale in the region and worldwide, Huawei believes that connectivity, cloud, AI, computing, and industry applications are now truly coming together to create unprecedented opportunities for society. Huawei is thus focusing on applying ICT technologies to more industries through scenario-specific solutions that help enterprises to enhance their business, and governments to achieve strategic goals related to domestic productivity and improving overall governance.

Charles Yang, President of Huawei

Middle East, said, "This year's GITEX Technology Week comes at a time when the true value of ICT has become increasingly clear. Keeping people, businesses, and communities connected even when physically apart is more essential than ever. Through open collaboration, the ICT sector can accelerate the development of the digital economy, in turn contributing to sustainable growth and supporting national transformation agendas in a post-pandemic world."

GITEX visitors will not only see a demonstration of new technologies, but current and future-oriented applications that Huawei has developed with its global partners for customers in government, energy, transportation, finance, and more.



AVAYA TO ENABLE ORGANISATIONS MAKE EVERY EXPERIENCE MATTER

NIDAL ABOU-LTAIF, AVAYA INTERNATIONAL

enables remote visitors to experience the event from the comfort of their homes and offices.

Under the theme 'Every Experience Matters', the technologies on display are based on Avaya's multicloud application ecosystem that delivers effortless, seamless, and context-driven experiences across all touchpoints for customers and the employees who serve them.

At GITEK, Avaya will address the challenges of the new normal with a solution portfolio, powered by AI, automation and layered innovation, that enables businesses to create the future customer experience centre and future digital workplace and realize shorter time to value.

"The world is very much adapting to new business models – a fact made obvious by GITEK Technology Week's decision to adopt a hybrid approach

for its 2020 edition. COVID-19 has accelerated digital transformation by several years, and amid that shift, it's become clear that increased focus needs to be placed on delivering incredible experiences across every touchpoint. We'll be at GITEK to demonstrate how every experience matters, felt by a customer or employee and whether it's online or in-person. And that prioritizing those experiences is the key to business success in the new future of work," said Nidal Abou-Ltaif, President, Avaya International.

At the heart of Avaya's presence at GITEK is Avaya OneCloud, a unique hybrid delivery architecture that protects investments, prevents disruption, and ensures multiexperience continuity across each phase of a personalized cloud journey.

Visit Avaya at Stand Z1-B10, Zabeel Hall.

Avaya has announced its participation at the 2020 edition of GITEK Technology Week, where the company will demonstrate solutions that address post-pandemic business challenges and prepare organizations for the new world of work.

Avaya's presence at GITEK Technology Week, the only in-person global technology exhibition of 2020, will be supplemented with a large footprint on GITEK Unlimited, a digital platform that



SOLARWINDS TO SHOWCASE LATEST PRODUCT UPDATES

SASCHA GIESE, SOLARWINDS

At the event the company will showcase its latest innovations that provide an easier way to monitor SD-WAN connections and enhanced support for network automation to Python. SolarWinds will also demonstrate how its products can help enterprises transform from securing the perimeter to a zero trust model, which is crucial for any business in digital transformation.

Speaking about the importance of the tech show, Sascha Giese, Head Geek, SolarWinds, said, "GITEK is the number one technology show for the region, but even on a global scale it's a big show and

not to be missed. It's an important platform for us as each year we meet with existing customers and hear their latest stories, and we learn a lot from them! Even if this year it means we are meeting virtually."

According to Giese, SolarWinds' solutions were able to withstand the impact of the pandemic. "Even before the pandemic our solutions were ready to be deployed in any model – on-prem, hybrid, or pure cloud. Various features turned out to be extremely useful for the 'new normal,' for example VPN monitoring, or the ability to verify the connection in multi-cloud environments."

IT management software provider, SolarWinds, will exhibit the new releases and the latest updates to its offerings at GITEK Technology Week, which will also feature GISEC..



STARLINK TO PRESENT ITS BOLD 'CONNECT STRATEGY'

NIDAL OTHMAN, STARLINK

StarLink is set to participate in this year's GITEX Technology Week where it will showcase powerful technologies.

Amidst a global pandemic, StarLink continues in their unwavering leadership role, innovating with latest technologies, and connecting vendors with partners and customers in the Cybersecurity, Cloud and Data Centre

domains. This GITEX, StarLink has selected cutting-edge technologies namely Palo Alto Networks, Citrix, BeyondTrust, SailPoint, Nutanix, Infoblox, FireEye, Riverbed, Imperva, Forescout, Cloudera, Cofense, ThreatQ, Pulse Secure, FireMon, Getvisibility, LinkShadow, SecureLink and Tripwire - that are going to be essential for enterprises as they adapt to the new-normal.

StarLink and their participating vendor teams will be engaging and networking, both virtually and face-to-face, with channel partners and end-customers to share business and technical insights on their solutions offering and industry best practices.

"This year has been exceptional - full of learnings and new experiences.

With a 'new norm' being introduced, innovative ways of doing things has become inevitable. This has unlocked huge potential in the areas of digitization, cloud, AI and applications and we are excited about the opportunities presented by these changes. In line with our theme and strategy for FY'21 "StarLink Connect", we have invested in giving vendors, partners and end-users more ways to connect with experts from around the globe virtually, and face-to-face at our stand this GITEX. Every GITEX, StarLink raises the bar and this year will be no different," said Nidal Othman, co-founder & managing director, StarLink.

Visit them at Hall 2 entrance in the Enterprise and Security Arena.



SMART DUBAI TO SPOTLIGHT SMART CITY INITIATIVES AT GITEX 2020

YOUNUS AL NASSER, SMART DUBAI

them and move forward with digital development plans.

This year's event coincides with Smart Dubai's fifth anniversary, and the entity's participation is set to shed light on the progress it has made in its mission to transform Dubai into the world's smartest and happiest city, as well as the advancements recorded across various strategic digital transformation plans and projects.

Smart Dubai will also be looking to underline the importance and role of technology in facilitating people's lives and supporting various city sectors. Several government entities will be joining Smart Dubai's pavilion to showcase their existing and new services.

"GITEX Technology Week presents a prominent international platform that brings

together leading global figures from the technology and smart city sectors to discuss and exchange ideas," said His Excellency Younus Al Nasser, Assistant Director General of Smart Dubai, and CEO of the Dubai Data Establishment. "It is an ideal opportunity for governments, companies, and individuals to get a closer look at international smart city trends and explore best practices and success stories in the sector."

"We take part in this year's edition of the event as we celebrate the five-year anniversary of the establishment of Smart Dubai," H.E. added. "This makes us more determined to position Dubai as a leader in terms of smart cities, and as a city that has developed its own unique approach to providing innovative services and initiatives, employing advanced technologies to make people's lives easier and happier."

Smart Dubai will showcase the latest developments in the city-wide smart transformation of Dubai and the positive impact digitisation is making on people's lives.

Furthermore, Smart Dubai will be highlighting collaborative efforts undertaken in partnership with government entities when faced with the current global crisis, as well as the solutions developed to overcome

Huawei IdeaHub

New Style **Smart Office**

3-in-1 Whiteboard | Projector | Online Meeting



Scan QR code to Learn More



Frank Kim
Fellow Instructor,
SANS

ROADMAP TO CLOUD SUCCESS

AS THE CLOUD CONTINUES TO GROW AT A RAPID AND UNMITIGATED PACE, IT AND BUSINESS LEADERS NEED TO ENSURE THAT KEY PEOPLE WITHIN THEIR ORGANISATION ARE EQUIPPED WITH THE SKILLS TO EFFECTIVELY AND SECURELY LEVERAGE THE BENEFITS. SANS INSTITUTE FELLOW INSTRUCTOR **FRANK KIM** DISCUSSES HOW THE COMPANY'S LATEST CURRICULUM CAN ENABLE ENTERPRISES TO FUTURE-PROOF THEIR CLOUD STRATEGIES.

It is undeniable that many organisations start their journey to the cloud with cost optimisation as the primary goal. However, they soon realise that beyond cost-savings there's a plethora of benefits that they can gain, key among which is the capability to drive innovation.

The shift to the cloud enables enterprises, no matter the size or industry, to develop novel ways to bring products and services to market much faster.

Over the last few years, the cloud has evolved from being an industry buzzword to a catalyst for digital transformation. Cloud is enabling a whole host of innovations, enabling organisations to thrive and stay competitive amid the increasingly digital ecosystem. However, while the shift to the cloud presents boundless opportunities, it is not without its challenges.

According to recent industry studies, organisations often face the challenge of having to deal with misconfigured cloud platforms, which poses big security threats. Such bottlenecks are often attributed to the lack of cloud security talents within enterprises today. In fact, a report by US-based cloud computing firm Logicworks noted that 86 percent of IT decision-makers believe that the shortage of talent is slowing down their cloud initiatives.

This highlights why it is imperative for organisations to ensure that their security teams have the right talents that will enable them to efficiently and securely harness the value of the cloud.

To help modern enterprises cope with the growing challenges and provide IT teams with the right skills and knowledge, global information security training and security certification SANS Institute has launched a robust cloud security curriculum.

"The cloud makes it immensely easier for anyone to deploy new services. This increases the opportunity for shadow IT to arise and exacerbates the possibility that sensitive data may be stored and used in unknown or inappropriate ways. The lack of proper knowledge of cloud capabilities leads to cloud misconfigurations and insecure use of services, resulting in data breaches, reputational damage, and potential fines," says Frank Kim, Fellow Instructor, SANS Institute.

Cloud computing has become a major defining factor in the current and future state of information security, with the business reasons for moving to the cloud simply too overwhelming to ignore. 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.

"Just as the web defined the last 20 years of technology change, the cloud will be the defining element of the next

20 years,” says Kim. “Security must be part of this evolution in order to succeed. In terms of industry momentum, we’ve now reached the point where every cybersecurity professional needs to be knowledgeable about the cloud. This means that security professionals must focus on where the cloud is going, not where it is today.”

Kim, who is also the founder of security consulting and CISO advisory firm ThinkSec and the lead for the SANS Cloud Security curriculum, highlights that to succeed in cloud security organisations need talents that have hands-on technical experience and cloud security-specific knowledge. “IT and security professionals today must be prepared not only for their current role but also for a cutting-edge future in cloud security,” he adds.

Organisations today are adopting DevOps practices to get features and functionality to market faster that will enable them to take full advantage of the cloud. However, security often struggles to keep up. Additionally, with the rapid adoption of cloud services and platforms, it is now more pertinent than ever for security teams to understand the techniques and tools that will allow them to effectively monitor their environments for malicious activity.

To help IT and security professionals find the best starting point, SANS Institute has created a Cloud Security Flight Plan that will help them progress in their professional cloud security journey:

Baseline – Courses that impart the baseline skills required of any information security professional

involved in Cloud Security, whether active practitioner or manager

Foundational – Courses that provide the basic knowledge to introduce students to a required skill set for the Cloud Security industry as a whole.

Core – Courses that prepare professionals for more focused job functions in Cloud Security, including manager, architect, engineer, analyst, and developer.

Specialisation – Courses for critical, advanced skills, or specialised roles in Cloud Security

Management – Courses for leaders, managers, directors developing a cloud security roadmap, plan, procurement models, and ensuring policy and procedure are defined to support cloud

The flight plan includes the following courses:



LONG COURSES



SEC488: Cloud Security Essentials
License to learn cloud security.



SEC510: Public Cloud Security: AWS, Azure, and GCP
Multiple clouds require multiple solutions.



SEC522: Defending Web Applications Security Essentials
Not a matter of “If” but “when.” Be prepared for a web attack. We’ll teach you how.



SEC540: Cloud Security and DevOps Automation
The cloud moves fast. Automate to keep up.



SEC545: Cloud Security Architecture and Operations
In the cloud, no one can hear you scream. Architect it properly and you won’t have to.



SEC584: Cloud Native Security: Defending Containers & Kubernetes
Deploy securely at the speed of cloud native.



SEC588: Cloud Penetration Testing
Aim your arrows to the sky and penetrate the cloud.

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud
Stop treating the symptoms. Cure the disease.

SHORT COURSES



SEC534: Secure DevOps: A Practical Introduction
Principles! Practices! Tools! Oh my. Start your journey on the DevSecOps road here.



SEC541: Cloud Security Monitoring and Threat Hunting
Attackers can run but not hide. Our radar sees all threats.



MGT520: Leading Cloud Security Design and Implementation
Building and leading a cloud security program.



"In the cloud, all things are dependent on applications, code, and automation. As such, we have augmented our curriculum to deliver a more holistic approach to cloud security," explains Kim.

Many security professionals today are well-versed in traditional security tools and techniques. But as networks rapidly expand to include the cloud, the challenges are becoming even more acute.

"Our curriculum has been developed through an industry consensus process and is a holistic approach to address

"IT AND SECURITY PROFESSIONALS TODAY MUST BE PREPARED NOT ONLY FOR THEIR CURRENT ROLE BUT ALSO FOR A CUTTING-EDGE FUTURE IN CLOUD SECURITY."

the gaps in cloud security," says Kim. "This includes multi-cloud and hybrid cloud scenarios for the enterprise and developing organisations alike. They need to understand that they should not only learn the ins-and-outs of one platform, as the future demands in-depth technical abilities coupled with security knowledge for each big cloud service provider."

Kim also points out that with the development of the larger curriculum, SANS has conscientiously looked at job roles, training needs within those



roles and how they can help students progress even further in the future.

“Our curriculum offers a comprehensive approach to cloud security,” he explains. “Our courses range in complexity for those new to the cloud as well as those who have been around for the block a few times. If you are a developer, an architect, an

engineer, an analyst, a manager or a new security professional, the SANS Cloud Security Curriculum has the right content and training for you.”

Looking ahead, Kim says security professionals across the globe can expect new courses, certifications, and free resources such as posters, cheat sheets, whitepapers and webcasts. 📌

“THE LACK OF PROPER KNOWLEDGE OF CLOUD CAPABILITIES LEADS TO CLOUD MISCONFIGURATIONS AND INSECURE USE OF SERVICES, RESULTING IN DATA BREACHES, REPUTATIONAL DAMAGE, AND POTENTIAL FINES.”

UPCOMING COURSES

SEC388: Introduction to Cloud Computing and Security

SEC557: Continuous Automation for Enterprise and Cloud Compliance

FOR509: Cloud Forensics and Incident Response

www.sans.org/cloud-security

UPCOMING EVENT
CLOUD SECURITY EUROPE 2021
- LIVE ONLINE

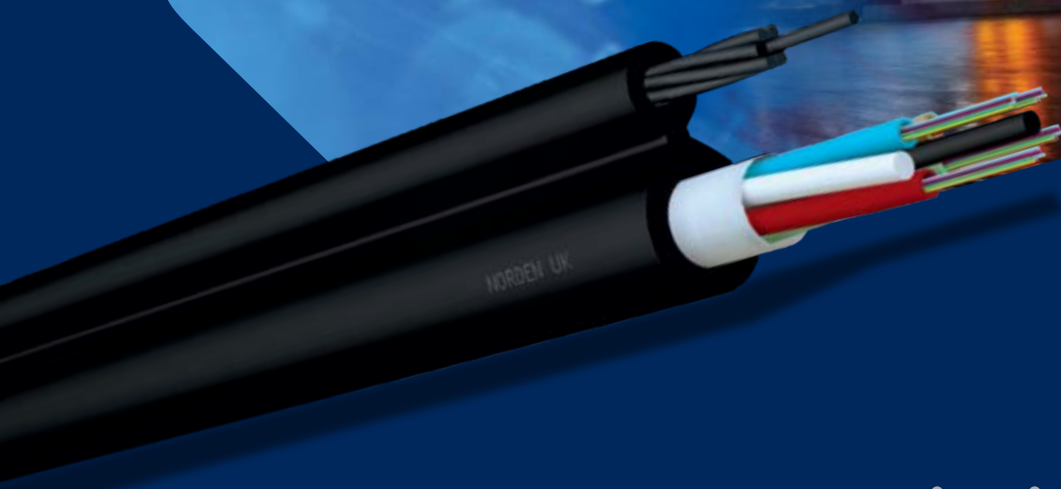
8th to 13th Feb 2021

<https://www.sans.org/event/cloud-security-europe-2021>



Reliable fast connection for all...

DIELECTRIC SELF-SUPPORTING FIGURE 8-AERIAL CABLE



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.



Norden Communication UK Ltd

Unit 13, Baker Close, Oakwood Business Park
Clacton-on-Sea, Essex, CO15 4BD, United Kingdom
Tel: +44 [0] 1255 474063, E-mail: support@norden.co.uk



www.nordencommunication.com

ESET: READY TO MAKE WAVES AT GITEX 2020

COMPANY TO SHOWCASE RECENTLY LAUNCHED PRODUCTS AT EVENT,
SAYS DEMES STROUTHOS – GENERAL MANAGER, ESET MIDDLE EAST.

What is the primary highlight of your participation at this year's GITEX?

This year at GITEX Technology Week, ESET will showcase a series of recently launched products which would include ESET Cloud Office Security, ESET Remote workforce offer, and ESET Targeted Attack Protection.

Why is GISEC/GITEX an important platform for your company and how is your participation different from the previous editions?

ESET has been part of GITEX for past several years, it has always been a great platform for meeting and networking with channel partners, customers, industry experts, and other peers from all across the Middle East region. GITEX is also a perfect platform for launching new products, and creating brand awareness among large targeted audience in less time.

The major difference this year is that we will be running series of webinars and online engagements on other virtual platforms during the show to

highlight new features and advantage of our new products and product roadmap for the year 2021.

What do you think will be the most pertinent security solution in the new normal? And, why?

Multi-factor Authentication has become the most pertinent security solution in the new normal, as huge numbers of organisations have deployed large-scale remote working, while threat actors have increased their attempts exponentially.

How will your offerings be instrumental in enabling organisations become cyber resilient in the new normal?

With remote working becoming the new normal for employees, employees are using different endpoint devices as a regular part of everyday work. It is vital that these devices are protected. Businesses should ensure that all their endpoints are secured and ESET has a wide range of endpoint security solutions from antivirus to multi-factor authentication and more advanced solutions like threat hunting and cloud-based sandboxing which protect against evolving range of cyberthreats with their multilayered defense capabilities.

Our recently launched products ESET Remote Workforce Offer, a cloud-based console that uses advanced technology like machine learning, deep behavioural inspection & ransomware shield to protect business data and ESET Targeted Attack Protection, a powerful ransomware prevention solution that is augmented by ESET EDR and Cloud Sandbox Analysis are interesting new additions to our portfolio which we shall demo during GITEX that provide businesses with improved endpoint protection. 🗝



“THE MAJOR DIFFERENCE THIS YEAR IS THAT WE WILL BE RUNNING A SERIES OF WEBINARS AND ONLINE ENGAGEMENTS ON OTHER VIRTUAL PLATFORMS DURING THE SHOW.”

CONNECTING BETTER WITH CUSTOMERS

AT GISEC, GULF IT HOPES TO REGAIN ITS PRE-COVID MOMENTUM WITH ITS PARTNERS AND CUSTOMERS, SAYS SAM EMMANUEL, BUSINESS UNIT MANAGER.

What is the primary highlight of your participation at this year's GISEC?

This year's GISEC is a big step in the right direction for the region and for the industry. The push and intention has been to move towards ending the uncertainty around the events and businesses. Our idea for this year's GISEC is to get back the pre-Covid momentum which was momentarily slowed down by lockdown around the globe. We are hoping at reconnecting with our customers and partners as is the norm during the GISEC. We expect the conversations and discussions to be different in terms



“ADAPTABILITY IS THE KEY IN THE COMING MONTHS, THE TRENDS HAVE NOT TAKEN THE FINAL FORM IN TERMS OF HOW CUSTOMERS WANT THEIR BUSINESS FUNCTIONS TO TAKE PLACE.”

of information security considering how the people have had to adapt over the past year due to the restrictions.

Why is GISEC/GITEX an important platform for your company and how is your participation different from the previous editions?

GISEC/GITEX are something that we look forward to because of the sheer size of the platform that it provides. This year it is expected to be different as it should be for everyone's health and safety. But we do expect the things to pickup as we get started. The event is a sign of how we are effectively overcoming the pandemic safely as well. Although the footfall maybe is lesser due to travel precautions but it is our efforts that will eventually yield results. Even though the expected visitors are less the crowd we are expecting is much more focused.

Can you please share some of the highlights at the company over the past year?

2020 has been a year of transformation for Gulf IT and we have been very intentional about the being on our growth and transformation track even during the pandemic. We have proven ourselves over the past decade to customers and channel about our strengths and value we bring to the table. During 2020 our team

strength has grown to keep up with the increased demand from the market. We've on boarded several top notch vendors like Resolve, Swivel, Seclore and NNT for this year to add to our portfolio. We had been working with Sailpoint over the past year and all the efforts have been bringing in results for this year as well in all the regions. Our success with the major banks in the sector has continued to soar over the past year along with the increased engagement in the government sectors.

What do you think will be the most pertinent security solution in the new normal? And, why?

Over the past years the region has been hesitant to onboard cloud based solutions but I believe this process of cloud acceptance has accelerated because of the work environment that was forced upon us due to the pandemic. Now increased cloud adoption with data and services moving to cloud has forced customers to look out for cloud security as well. So over the next few years the cloud security market will be picking up along with the vendors in that space. We had very good demand with for Imperva and NNT this year along with Resolve systems which helps large enterprises with migration to cloud environment. We do see IAM solutions like Sailpoint playing a big role for customers in

managing users in their environment. The need for MFA has increased exponentially as well and we hope to see that continue as well as customers explore options. Adaptability is the key in the upcoming months, the trends have not taken the final form in terms on how customers want their business functions to take place but I believe over the next few months as this stabilises cybersecurity market will start coming up with some new trends as well. We do expect the upward trend to continue in the upcoming quarters.

How will your offerings be instrumental in enabling organisations become cyber resilient in the new normal?

Gulf IT has been a major player in helping customers onboard the latest and the greatest in technology. The past decade has been a proof of how we have been successful in achieving that. Our approach to customers have always been solutions rather than products. Our products are on boarded to complete or fill in the gaps of the solutions provided to customers. Even with our vendors we adopt a holistic approach to customer's pain points to ensure we address the roots rather than the symptoms. Especially with a lot of users logging in remotely the need to protect the data has become all the more important. For Data security Imperva, Seclore and NNT have been leading the pack and we hope to see it continue in the upcoming year. The increased team strength has helped us to gain market confidence in tackling the challenges put forward by the pandemic. Our round the clock support and technical expertise for customers has been appreciated and we intend to grow that support even more this year. 🙌



NAVIGATING THE NEW NORMAL

HUSNI HAMMOUD, MANAGING DIRECTOR BARRACUDA NETWORKS, IVANTI AND ESET MIDDLE EAST (PART OF MIDIS GROUP) SPEAKS TO SAME ABOUT THE NEW SECURITY LANDSCAPE POST THE PANDEMIC AND HOW INNOVATION CONTINUES TO REMAIN THE KEY TO FUTURE GROWTH.

How has the ongoing pandemic impacted attitudes and investments around security?

The coronavirus has definitely had a big impact on all of us, from every point-our lifestyle, operations etc-so much so that all this affected our way of doing business. At the same time, it created new areas of opportunity that had never been considered before, like remote working, for example. It forced us to ensure business continuity and communicate with our clients in more effective ways than before. In fact, the pandemic even forced us to re-orient our thoughts as well. All this created a new way of life, so of course, it brought with it its own share of

risks. These risks go back to the basic concepts of security, which are: availability, which means I need to be always in contact with people and reachable, and at the same time ensure the safety and security of communication between my company and the client, at the same time, I need to authenticate and ensure that the right people have access to the right information. On top of that, we have the IT infrastructure that needs to be adapted in order to fulfil all these requirements. Additionally, the IT people need to have the capabilities and tools in order to manage remote working and securing their servers, their cloud infrastructure, their networks and most importantly, their end point and mobile environment where everything needs



to be connected from anywhere. So, the pandemic has pushed all these requirements exponentially in a just few months, when normally it would take a few years to develop.

Over the last few months, we have seen a spike in threat actors targeting employees working remotely. How can organisations ensure that their workforce is security aware and is practicing good cyber hygiene while working outside corporate networks?

Most of the companies dealt with this aspect by focusing on training and

awareness. This is the most important aspect. People are not used to having everything online and communicating so much electronically. A lot of risks rose from this sudden spurt in online activity because now all websites look legitimate. So, if I click any website, and input my details, it becomes easy for hackers to access all our secure data and compromise on sensitive company information. Web conferencing and videos became important during the days of the pandemic and the lockdown because people had the time to watch and learn and train themselves with new and challenging developments. Companies and IT teams braced for the challenge by working on new solutions, so that everyone was ready by the time we emerged out of the lockdown. So, the sales of the infrastructure components from networking, servers and cloud subscriptions went up because people wanted to make sure their information is secure anywhere and everywhere.

The other thing is that companies had to secure their communications so a

lot of virtualisation and network access solutions were introduced, and there was a lot of growth in web applications, firewall and web security in order to ensure that online businesses are secure and accessible through the right people. So, these are the areas that most of the companies jumped into, from day zero.

Can you please share some of the highlights at the company over the past year?

I am managing a sub-group of local offices in MIDIS group which includes multiple vendors like Barracuda, ESET and Ivanti. All of them have cutting-edge solutions that cover email security, endpoint security, cloud and network security, etc covering the Middle East, Europe and Africa markets. We were ready from day zero to support and adapt to the pandemic situation. Firstly, we readied ourselves to work remotely and adapt to the new station, at the same time, we were also ready with our solutions to provide them with the necessary tools required during this time. So, we have a list of products that are available which cover all key aspects of modern technology such as cloud back up, patch management, remote management-all of which being part of our product portfolio. Overall, I think the pandemic period was a hectic one for everyone, but thankfully, we have the proper team and proper processes in place that helped us to be ready, on time, and we hope to continue on this promising note for the coming years, to provide new and inventive solutions for the region. 🙏

tahawultech.com CISO50 & FUTURE SECURITY AWARDS 2020

ON 24TH NOVEMBER, TAHAWULTECH.COM AND SECURITY ADVISOR ME HOSTED A VIRTUAL AWARDS CEREMONY, WHICH RECOGNISED ENTERPRISE IT SECURITY LEADERS AND ORGANISATIONS THAT HAVE DELIVERED REAL-WORLD RESULTS FOR DRIVING SECURITY TRANSFORMATION.

A

s the world continues to navigate the challenges and changes brought about by the ongoing COVID-19 pandemic, many organisations are realising the need to accelerate their digital journeys.

Over the last few months, businesses across multiple industries have fast-tracked their adoption of digital solutions. While this has presented numerous benefits for these organisations, it has also given threat actors the opportunity to exploit new vulnerabilities within IT systems.

If it wasn't clear before, it is becoming more apparent now more than ever that security is a key priority for businesses no matter their size, industry or where they are located.

It is also becoming more evident that the role of security leaders – whether it be the enterprise CISOs and IT security teams or security vendors – are becoming more integral in enabling organisations to continue to thrive, while staying resilient in the current landscape.

To recognise the excellent leadership that CISOs and IT security innovators have demonstrated over the past year, TahawulTech.com and Security Advisor ME hosted the CISO 50 and Future Security Awards last month.

The virtual awards ceremony celebrated 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.

The Awards welcomed organisations from across the Middle East. It acclaimed the best security minds and projects 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.

The CISO50 and Future Security Awards 2020 also featured a thought-provoking panel discussion on the topic, "Navigating the cybersecurity challenges of the new normal," which spotlighted top insights from Fadi Yehia, Sales Director for South Gulf, Fortinet; Omar Ben Hamadou, EMEA Sales Manager, Kapalya Inc.; and Ahmed Diab, Sales Director – Security Solutions, StarLink. 🔑

PANELLISTS



Ahmed Diab,
StarLink



Fadi Yehia,
Fortinet



Omar Ben Hamadou,
Kapalya Inc.



Abdul Rahman Hamdi Shelleh
AL DHAFRAH REGION MUNICIPALITY



Abdulla Bader Al Sayari
DEPARTMENT OF HEALTH - ABU DHABI



Dr. Ahmed Al Ketbi
DEWA



Ahmed Al Mutiri
NWC - THE NATIONAL WATER COMPANY



Ahmed Hassan Al Lawati
OOREDOO OMAN



Ali Juma Alajmi
MINISTRY OF HEALTH AND PREVENTION



Aliasgar Bohari
ZULEKHA HOSPITAL



Anoop Kumar
AL NISR PUBLISHING



Arif Irfani
SHARJAH ISLAMIC BANK



Ashish Khanna
DUBAI HEALTH AUTHORITY



Ayman Al Shafai



Bilal Ahmed Chaudhry
EMIRATES FLOAT GLASS LLC



Choudhary Muhammad Zia Ur Rehman
NATIONAL MEDIA COUNCIL



Dileep Raj Abdul Razack
DEPARTMENT OF MUNICIPALITIES
AND TRANSPORT (DMT)



Dr. Erdal Ozkaya
STANDARD CHARTERED BANK



Ebrahim Kamalzadeh
ALNABOODAH AUTOMOBILES



Eid Al Beer
MINISTRY OF INTERIOR



Eng. Khalfan Matar Al Hassani
ADMCC



Fatema Ahmed Almalki
RAK EGA



George Eapen
PETROFAC



Irshad Mohammed
VPS HEALTHCARE



Ismail Jani
ENGINEERING OFFICE



Jamil Rashdi
WASL ASSET MANAGEMENT



Jayesh Nandan
MEDICLINIC MIDDLE EAST



Jean-Michel Briffaut
SERCO



Jeevan Badigari
MAJID AL FUTTAIM VENTURES



Khalid al Faheid
MINISTRY OF ENVIRONMENT,
WATER AND AGRICULTURE (MEWA) -KSA



Kiran Awad
EXPORT TRADING GROUP



Manan Shah
BLACK WIT CYBER SOLUTIONS



Mario Foster
AL NABOODAH GROUP ENTERPRISES



Mazen Al Ahmadi
STC



Mohamed Alajmani
SHARJAH CUSTOMS



Mohammed Darwish Azad
EMIRATES NBD



Mohammed S. Dhawi
MINISTRY OF FINANCE - KSA



Muhammad Irfan Khan
TIGER GROUP OF COMPANIES



Munther Binamro
ABU DHABI QUALITY AND CONFORMITY COUNCIL



Mustansir Aziz
GULF DIAGNOSTIC CENTER HOSPITAL



Nithin Geo Thomas
AMITY EDUCATION



Prince Rana
AL FARDAN GROUP



Ramachandra Ullur
JOTUN UAE LTD LLC



Ravikumar Yogi
ABU DHABI DEPARTMENT OF FINANCE



Rotimi Akinyele
RAS AL KHAIMAH ECONOMIC ZONE -
GOVERNMENT OF RAS AL KHAIMAH



Saghir Ahmad
AL RAJHI BANK



Saju Plasseril Vasu
DUBAI NATIONAL INSURANCE & REINSURANCE P.S.C



Shabbir Nalwala
ISYX TECHNOLOGIES LLC (SANDS
INTERNATIONAL GROUP)



Shafik Riad Hasna
MINISTRY OF ECONOMY



Shah E Room Khan
EMIRATES COLLEGE OF TECHNOLOGY



Somnath Sarkar
MASHREQ BANK



Srinivas Mathala
OSN



Varun Vij
SERCO



Venu Sriraj
UAE EXCHANGE



Vivek Gupta
GEMS EDUCATION



Yaser Al Yousef
MINISTRY OF JUSTICE - KSA



Yousuf Marhoon
DUBAI AIR NAVIGATION SERVICES



Manivannan Nagarajan
MASHREQ BANK



tahawultech.com

CISO50 & FUTURE SECURITY AWARDS 2020

GAJSHIELD
Data Security Firewall

Best Cloud Security Vendor


cybereason

Best Endpoint Security Vendor

HIKVISION®

Best Internet of
Things Security Vendor

FORTINET®

Best Network Security Vendor

 **NORDEN®**

Best Surveillance Systems Vendor

 **Barracuda®**
Your journey, secured.

Best Enterprise Email
Security Solution

A10 Networks

Best 5G Security Vendor

 **Gulf IT**
Network Distribution

Best Cybersecurity Distributor

SANS
INSTITUTE

Best Cybersecurity
Training Provider

رقميات
Raqmiyat 

Best Disaster Recovery
Solutions Provider

 **EXCLUSIVE
NETWORKS**

Best Security VAD



Best Data Protection Vendor



Network Detection &
Response Vendor



Best Cybersecurity System Vendor



Best Email Security Vendor



Best SMB Endpoint
Security Vendor



Best Privileged Access
Management Vendor



IT Cost Optimisation
Service Provider



Best Innovative
Security Product



Security Transformation
Catalyst Award



Specialist Cybersecurity VAD



Best Security IAM
Integration Software

HOW CLOUD COMPUTING WILL ACCELERATE DIGITAL TRANSFORMATION IN A POST-EPIDEMIC ERA

LI SHI, PRESIDENT OF CLOUD AND AI BUSINESS GROUP, HUAWEI MIDDLE EAST, DISCUSSES HOW DIGITAL TECHNOLOGIES SUCH AS CLOUD COMPUTING AND AI WILL ENABLE ENTERPRISES TO SUCCEED IN A POST-EPIDEMIC ERA.

In 2020, the COVID-19 epidemic has brought a great impact on people's lives around the world. As a response to the impact, many enterprises are accelerating their digital transformation and maintaining business and production continuity through remote work and remote collaboration. Cloud-based collaboration software became ubiquitous during the epidemic, allowing billions of teleconferences to be held worldwide every day. Technology is critical to the survival of businesses, according to a new study by Global Data, a well-known research institution, with more than 80 percent of executives saying cloud computing and network are key to helping their businesses get through the crisis.

In fact, a perception is emerging in many industries that entrepreneurs have experienced a digital enlightenment during the epidemic. In the post-epidemic era, all industries will accelerate digital transformation, either actively or passively, to better adapt to future market challenges.

Healthcare has always been an important industry for everyone, especially this year. Cloud computing and AI technologies have been widely used by medical staffs in the fight against epidemics and vaccine development, providing great value for people's lives and health. Researchers are using cloud computing-based AI technologies to analyse vaccines in the US, Europe, and Asia, which can effectively shorten the vaccine development process. With

increasingly developed communications network technologies, patients can access the healthcare cloud anytime, anywhere to obtain transparent, customisable, and cost-effective healthcare solutions and evaluate healthcare outcomes. Cloud computing is helping the healthcare industry move towards value-driven and consumer-centric patient care.

The transport industry is also a very typical example. Under the tide of economic globalisation, large cities in various countries are becoming an important part of the world's urban system, and some international metropolises have become global productive forces, science and technology centres, educational and cultural centres and world trade centres. However, with



the influx of population, large cities face more and more challenges in traffic management, which are difficult to solve by traditional means.

In many large cities around the world, traffic management departments are trying to improve the traffic conditions of cities by using various technologies, including updating intelligent traffic sensing devices to obtain clearer and more accurate traffic data. Building a unified traffic management system based on a cloud computing platform can coordinate the handling of traffic signals and emergency cases. Using multiple connection technologies, including 5G, will also optimise data connections between traffic sensing devices and the traffic management system, ensuring that massive data can be aggregated and analysed in a timely manner. Advanced AI analysis algorithms can in turn analyse and support decision-making for

congestion prediction, route analysis, and traffic signal control, then, the analysis result and decision-making suggestions could be sent to the traffic control department and frontline traffic police through the network. The integration of these new technologies effectively improves the urban transportation environment.

In addition to improving benefits for traditional industries and large-scale enterprises, emerging digital technologies such as cloud computing and AI will also provide new opportunities for small and

medium-sized enterprises to improve operation efficiency, promote innovation, expand market and financing channels, and facilitate remote operations during the epidemic. In the Middle East, SMEs account for more than 90 percent of the total size of enterprises and contribute 70 percent of GDP. Helping small and medium-sized enterprises accelerate their digital transformation will bring significant benefits to local economic development.

Now, with the development of vaccines in various countries, the epidemic will gradually be effectively controlled. As businesses move from addressing the COVID-19 epidemic to driving sustained business growth, they must focus on the three main areas that shape the trend this year: consumer-oriented, business independence, and intelligent delivery. These trends will have a greater impact when combined, and businesses must focus on meeting social and individual needs around the globe for optimal practice.

Digital transformation is entering the next stage as 'intelligence', which is the key strategy for the future development of global cities, industries and enterprises. From research by Gartner, a leading research firm, shows that the need for business resilience has never been more intense. CIOs are trying to adapt to changing circumstances and design future-oriented businesses. This requires that the enterprise organisation be sufficiently intelligent and reorganised and reformed plasticity.

The intelligent business architecture and anywhere operations mode that is implemented based on the cloud computing platform, AI, 5G, and IoT technologies is the key to future enterprise development. Only companies that take advantage of the combination of these technologies for continuous digital transformation will have the chance to be the winner of business competition over the next few years. 📌

“DIGITAL TRANSFORMATION IS ENTERING THE NEXT STAGE AS ‘INTELLIGENCE’, WHICH IS THE KEY STRATEGY FOR THE FUTURE DEVELOPMENT OF GLOBAL CITIES, INDUSTRIES AND ENTERPRISES.”





A Bright Idea for Your Home

Traditional floodlights offer very limited functionality. Enhance your security by adding surveillance, real-time response and more.

EUFY SECURITY: SMART FLOODLIGHT WITH CAMERA

Time to Upgrade Your Floodlights: Traditional floodlights offer very limited functionality. Enhance your security by adding surveillance, real-time communication via 2-way audio, and more.

Drop-in Anytime

in 1080p: Live-stream and record in full 1080p HD so you can see exactly who's there in crisp clarity.

No Hidden Costs: Designed to protect your home as well as your wallet, eufy Security products are one-time purchases that combine security with convenience.

Turn Night Into Day: 2,500-lumen super-bright motion-activated floodlights deter intruders and ensure detailed, full-color recordings even at night.

Smart Siren: A harsh warning for any intruders. A loud 100dB alarm can be triggered to scare off any unwanted visitors.

FROM EUFY, THE HOME SECURITY BRAND WHERE PRIVACY COMES FIRST.

- Comprehensive Safety Solutions for Your Home

- Created by the same team as Anker—renowned for exceptional quality and innovation

PROTECTS YOU, YOUR FAMILY, AND YOUR PRIVACY

Every eufy Security product is engineered to ensure your security data is kept private. Have peace of mind that you will have a secure record of everything that happens around your home.

EVERY CORNER COVERED

Wide-angle view ensures you get the whole picture while streaming in full 1080p HD.

2,500 LUMENS BRIGHT

Light up every corner and scare off intruders when motion is detected.

"Alexa, show me my garage door"

Connect your Floodlight to Alexa or Google Assistant and check-in anytime on what's happening outside your home. 🏠



<https://www.eufylife.com/products/variant/smart-floodlight-with-camera/T84201W1>

Available at Sharaf DG, Jumbo, Lulu, Amazon and noon

SANS CLOUD SECURITY

SANS believes that the cloud is a transformative technology that will define the technology landscape for many years to come. Given the unmitigated growth of Cloud, we have launched the Cloud Security Curriculum to give you the training and skills you need to become a cloud security expert. There are SEVEN new cloud security courses being launched in 2020 with several more planned for 2021.

LONG COURSES

SEC488: Cloud Security Essentials

Learning the language of Cloud Security.

SEC510: Multicloud Security Assessment & Defense

Multiple clouds require multiple solutions.

SEC522: Defending Web Applications Security Essentials

Not a matter of “if” but “when”. Be prepared for a web app attack. we'll teach you how.

SEC540: Cloud Security & DevOps Automation

The cloud moves fast. Automate to keep up.

SEC545: Cloud Security Architecture & Operations

In the cloud, no one can hear you scream. Architect it properly and you won't have to.

SEC588: Cloud Penetration Testing

Aim your arrows to the sky and penetrate the Cloud.

SEC584: Cloud Native Security: Defending Containers and Kubernetes

Deliver securely at the speed of cloud native.

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

Stop treating the symptoms. Cure the disease.

SHORT COURSES

SEC534: Secure DevOps: A Practical Introduction

Principles! Practices! Tools! Oh My! Start your journey on the DevSecOps road here.

SEC541: Cloud Security Monitoring and Threat Hunting

Attackers Can Run But Not Hide. Our Radar Sees All Threats.

MGT520: Leading Cloud Security Design & Implementation

Building and leading a cloud security program.

“I am very happy that I chose to take this class. The course content is amazing. I am getting great perspectives to help me map my traditional engineering skills to cloud skills. I have found that the labs helped me immediately apply what I learned to my new role.”

Lemanuel Williams, Red Canary (SEC545 Student)

To find out more about Cloud Security Courses,
visit sans.org/study-cloud-security

THE QUICK AND THE DEAD: FUTURE-PROOFING SECOPS

SAM CURRY, CHIEF SECURITY OFFICER, CYBEREASON, DISCUSSES HOW CYBER ADVERSARIES ARE EVOLVING THEIR METHODS AND WHAT IT WILL TAKE FOR ENTERPRISES TO FUTURE-PROOF THEIR STRATEGIES.

The quick and the dead is an English phrase from William Tyndale's translation of the New Testament. The word quick, in English, comes from the old Anglo Saxon for alive, and nothing could be more apt. To be quick is to be alive, and nowhere is this more true than in security where we literally are in a race, albeit an asymmetric one, against an intelligent, adaptive opponent. For this reason, security is about ultimately about rates.

The adversary is innovative, motivated, funded and enjoys the advantages of asymmetry — they only have to be right once to succeed, while the defender has to play a perfect game. Given the focus and investment, the rate of improvement in the proficiency of attackers is increasing faster than, by-and-large, that of the defenders. The first step to being futureproofed is to be present-proofed; and the essence of that is to be quick and adaptive and to seek to maximize the incremental improvements

and the pace of advancement. In a word, security needs to be more agile with people, with processes, and with technology.

Using the word agile, however is a loaded term in technology because it is at the heart of the DevOps revolution, writing better and more sustainable code and owning code in production as much as in the back office. For many, the agile R&D movement can feel a bit revolutionary or even cultish. It is, after all, a complete change in how



“ANYTHING WE DO THAT IS STATIC AND PREDICTABLE CAN BECOME A LIABILITY.”

engineering is done, shifting to user centricism, owning production code, and an emphasis on pragmatism in what we now call DevOps. The agile manifesto, though, has extremely valuable lessons and can lead to a similar revolution in SecOps if we apply the principles correctly — the user isn't to blame, policies have to account for real human behavior, a focus on processes, owning results, a dedication to incremental improvement, working policies, collaborating on with the business, responding to change. In

this world, perfection is the enemy of the good to paraphrase Voltaire, and incremental improvement is at the heart of accelerating how effective security operations are.

As an example, Indicators of Compromise (IOC) are no longer the star in the fight to detect and prevent advanced attacks as we have had opportunity to learn time and again and most recently in Operation SoftCell. In SoftCell, every instance of malware, from China Chopper to the now venerable Poison Ivy, had a unique signature. Every single time it was used and placed in the victims' environments, it had a unique signature. This meant that finding it in one place did nothing for finding it again, and checking public sources with the file hash became a feedback loop that actually helped the bad guys know what machine was potentially the battleground and a lost asset. In other words, IOCs can be a liability and made to work against us.

The adversary is always on the attack and has effectively found ways around IOCs. The only time an IOC bell rings is either when the attacker makes a

mistake or when they intentionally drive a diversion to increase noise-to-signal ratio. There will always be a role for IOCs in reducing noise, stopping the low-hanging fruit of the threat world, tuning out noise and adding color to security operations; but security is a chaotic system with an intelligent opponent. Anything we do that is static and predictable can become a liability. This might seem the antithesis of most process management, but it's not. It's just the new reality for operations and one that we can adapt to if we focus on being adaptive as a core principle.

The heart of future-proof security operations is a lean-in, detection mindset; an agile methodology; and a dedication to incremental improvement. This inevitably leads to new behavioral telemetry sources like EDR and its successor XDR, to decrementing “just capture it all” from the SIEM years and to an emphasis on reliable and hard-to-predict-by-attackers automation. This is the path to a world where the attackers only have to get it right once to a world where they have to be right all the time and still expect to fail. 🕯



“ENCRYPTION IS NON-NEGOTIABLE”: KAPALYA

MOHAMED MENAKBI, VP SALES & STRATEGIES – EMEA, KAPALYA, DELVES INTO THE IMPORTANCE OF ENCRYPTION IN KEEPING DATA PROTECTED AND IN SECURING ENTERPRISES.

Can you please share a brief overview of Kapalya Inc?

Kapalya develops solutions that offer enterprises with an innovative approach to the management of user encryption keys. We have a unique technology reduces the risk of data being compromised. Kapalya is a part of by Caltrop Cybersecurity, the security arm of US-based technical management support services firm Caltrop.

We have a presence across Europe, the Middle East and Africa. We have a direct business here in the UAE and Saudi Arabia. We have 113 employees deployed across the UAE and Saudi Arabia most of who are part of the service desk, deployment and project management, quality assurance advisory and more. And we also have an indirect business, through our partners, in markets such as Oman, Kuwait and Levant.

“AT KAPALYA, WE DO THE HEAVY LIFTING FOR OUR CUSTOMERS. WE PROVIDE THEM WITH A COMPREHENSIVE SOLUTION THAT’S USER-FRIENDLY FOR BOTH END-USERS AND ADMINISTRATORS.”

How has the ongoing pandemic impacted attitudes and investments around security?

We have seen a huge increase in cyber threats since the start of the COVID-19 pandemic. This is primarily driven by the increase in the number of organisations implementing remote working schemes. Employees that are working from home are using unsecured devices such as laptops, mobiles and tablets. Many of them are accessing corporate networks from their home WiFi that may not be secured. This puts enterprise networks at great risk of being infiltrated by threat actors by hacking the resources of unwitting employees.

Additionally, there are employees from across multiple departments accessing enterprise applications for HR, logistics, accounting and so on from unprotected devices and are sharing data over potentially unsecured channels.

Fortunately, members of the C-suite – whether it be of a school, bank or private enterprise – are increasingly realising the implications of such scenarios and are now paying attention to securing their remote applications and their corporate data that resides in the cloud.

As more companies migrate to the cloud, they need to also invest in cloud security. Can you please elaborate on the importance of encryption in

ensuring the success of cloud security strategies?

Many organisations are investing in the cloud with the primary goal of reducing their OPEX and streamlining their IT infrastructure. However, what they need to realise is that the responsibility of securing their data is still with them.

Encryption is a key element of comprehensive data-centric security. As more and more organisations leverage the cloud technologies as part of their remote working schemes, they need to protect sensitive data in-transit and at-rest on their public and private cloud environments.

At the same time, most businesses run hybrid IT environments with applications that are on-premise and in the cloud. End-to-end encryption ensures data protection regardless of whether corporate data is in a public or private cloud, on a device, or in transit.

How can organisations implement the right data protection and encryption methods without stifling productivity? How can Kapalya enable their success in this space?

While organisations may have invested in firewalls and other cybersecurity upgrades at the office, due to current the workplace dynamics employees may no longer have access to these resources.

Encrypted data can only be opened by someone who has the right access or ‘key’. This way, even if a threat actor intercepts a company file or critical data, they would be unable to open it. However, what often stifles productivity are solutions that are too complex or have features that are unfriendly to users. At Kapalya, we do the heavy lifting for our customers. We provide them with a comprehensive solution that’s user-friendly for both end-users and administrators.

Kapalya offers a unique approach to encryption key management. We provide customers with a full-service encryption solution that protects data by seamlessly encrypting files on endpoints, mobile, corporate servers and public clouds. We made the whole process simple and seamless. This is because we believe that for any organisation cybersecurity is mandatory and encryption is non-negotiable.

Where do you see the cybersecurity landscape heading in the next few months? What can the market expect from Kapalya?

Cybersecurity will always be the number one priority for organisations. Subsequently, with data residing everywhere, whether on-prem, public cloud or private cloud, protecting that data will become more critical than ever. Additionally, we predict that cybersecurity will also become smarter, thanks to trends such as artificial intelligence (AI) and machine learning.

For Kapalya, we have a very strong roadmap into implementing more AI and automation features into our solutions. Looking forward, we are looking at developing encryption solutions to endpoints such as smart buildings, drones and more. 📌

CYBERSECURITY 2021: THE NEW YEAR WILL BRING NEW CHALLENGES

WITH ATTACKS ON THE RISE AND A LARGER-THAN-LIFE SURFACE TO DEFEND, SECURITY TEAMS WILL NEED A NEW MINDSET IN ORDER TO KEEP THEIR SYSTEMS, DATA AND PEOPLE SAFE, SAYS CITRIX'S CHIEF INFORMATION SECURITY OFFICER **FERMIN SERNA**.

Defending corporate systems and information has never been easy. But the global pandemic has complicated things in ways no one could have predicted and is accelerating trends that promise to upend the way organisations think about and approach security in the year ahead. What will things look like in 2021? In a world where figuring out what will happen today is all but impossible, it's hard to say what the future holds. But a few things are clear:

Remote work is here to stay

At the outset of 2020, remote work was something most companies were experimenting with. But mid-way through

the year, things got serious as COVID-19 began to spread and mandates forced the masses to work from home. While many companies viewed remote work as a short-term solution to the pandemic problem, they are now realising that it is here to stay. Research shows that over three-quarters of more than 3,700 IT leaders in seven countries believe most workers will be reluctant to return to the office post pandemic. And they will need to revamp their security policies to support them as they work from anywhere.

There will be no perimeter

Three years ago, everything was on prem and the security perimeter was defined by firewalls. Today, applications and

services are rapidly moving to the cloud, people are working from anywhere and the perimeter has all but disappeared. Corporate information security teams will no longer rely on traditional, VPN-based strategies to provide access. Instead, they will shift to a Zero Trust model that uses contextual awareness to adaptively grant access based on user behaviours and access patterns.

Experience will influence strategy

In a recent survey conducted by Citrix and Pulse, 97 percent of 100 IT decision makers in North America, Europe, the Middle East, Africa and the Asia Pacific region said employee experience is a key influence on their security strategy.



they need and prefer to use in a simple experience that can be customised to fit personal preferences and evolving work styles.

Cyber actors will become more sophisticated and scale

New ways of working mean new ways of attacking corporate networks. Ransomware and other malicious attacks are on the rise, with cybersecurity researchers reporting a seven-fold increase in malware campaigns at the mid-point of this year. Flush with cash from their demands, bad actors, have been empowered to scale their operations. And they will. Attacks will continue and become more sophisticated and dangerous.

Security will get smarter

As attackers get smarter and scale, security will get smarter

**“AS ATTACKERS
GET SMARTER
AND SCALE,
SECURITY WILL GET
SMARTER AND MORE
CREATIVE AS WELL.”**

And 75 percent said they are looking to improve the user experience through their design and execution. Security teams will take an intelligent, people-focused approach to security that protects employees without getting in the way of their experience by securing all tools, apps, content, and devices

and more creative as well. Machine learning and artificial intelligence will deliver real-time insights into user behaviour and access patterns, and security teams will use them to automate the process of identifying security incidents, atypical activity and policy violations and defend across gaps.

Vendors will get a closer look

The data chain is longer and more complex than ever. And with the perimeter gone, companies need to think beyond protecting their own systems and data and closely monitor all third-parties with whom they interact, as all it takes is one weak link to create a breach. With corporate brands, customer trust and business continuity at stake, security teams will place more scrutiny on their vendors and select only those who meet the highest standards for data privacy and protection.

CISOs will become more agile

Companies are rapidly moving to simplify and shift things to the cloud. And CISOs are adapting to secure the new environment. But ten years ago, there was no cloud. And five years from now, there will be something else. CISOs will become more agile in adapting to changes as technology evolves in 2021 and align closely with business leaders to provide a secure environment that fuels innovation and growth.

Looking ahead at a time when things have never been more uncertain may seem like a futile exercise. But there are lessons to be learned today that can help shape a better tomorrow. Just like work, cyber-attacks can happen anywhere, anytime. And in order to successfully protect the systems and information people need to get things done, wherever they happen to be, security organisations need to become more intelligent and flexible. In doing so, they can create the secure environments needed to keep employees engaged and productive and fuel innovation and business growth. 🗝️



DEFENDING THE HYBRID LANDSCAPE

BEN CARR, CHIEF INFORMATION SECURITY OFFICER, QUALYS, DISCUSSES WHY ENTERPRISES NEED TO UPDATE THEIR CYBERSECURITY BEST PRACTICES TO PROTECT THE NEW HYBRID WORKPLACE.

Although it is hard to imagine right now, we will enter a post-COVID-19 world — we shall emerge from our cocoons to be faced with the question of what we do next. The pandemic forced us to experiment at scale with technologies that were previously mere curios. Remote working has allowed entire economies to mitigate the rigours of the coronavirus, and across the Middle East, enterprises are discovering that operations can tick along quite efficiently under the new normal.

The UAE government has long made it clear it is in favour of a surge in remote working. The Ministry of Human Resources and Emiratisation has cited benefits such as reductions in

transportation expenses, pollution and traffic congestion, as well as more job opportunities for those living in remote areas. Just this past March, in the very early days of the pandemic, Statista reported that more than a third of Gulf companies (35 percent) were open to remote working. Around half of these (18 percent) were already working remotely and the other 17 percent were either considering it or were starting soon. Necessity being the mother of invention, COVID accelerated this migration.

So, if remote working is here to stay, should we not be establishing new policies to cope with the hordes of bad actors we know are still out there? You can be sure that they know the old ways are unfit for purpose; and you can also be sure they know those ways are still in use.

Make a list

New best practices are required to ensure everyone can work wherever, whenever, and however they need to. For a start, asset management should be prioritised. Remote workers give rise to unwieldy hybrid environments of cloud storage, containerisation, personal devices and unvetted public networks. With an always-accurate inventory you can at least identify weak points more easily and formulate action plans to address them. Otherwise, you are in the dark, waiting for the inevitable breach. When you consider this scenario and the potential catastrophes it portends, you can appreciate how the phrase "Shadow IT" was coined. It always sounded ominous, and for good reason.

Today, IT asset management is largely



Instead, you need to form a priority list of fixes that accounts for how easy the flaw is to exploit and how damaging the resultant penetration could be. Each business will have its own nightmare scenarios, and its own critical apps and data.

Get your priorities straight

Modern vulnerability management also needs to consider the pace at which the network changes. In the hybrid-working world, there is a perpetual revolving door of devices joining and leaving the corporate network, each with their own holes waiting to be patched. A priority framework will address all of this and rank vulnerabilities, meaning

resources will not be wasted on addressing the more trivial issues. Doing

rise, according to analysts around the world, but operational efficiency will still be expected by enterprise leadership teams. Automation of humdrum tasks is vital so that trained professionals can concentrate on the kinds of threats that call for uniquely human qualities like judgement and instinct. When freed up to attend to these trickier scenarios, security professionals can better demonstrate their worth.

The shifting frontier

But because we live in a world forever changed, and because we can expect the workplace to remain in this hybrid state for the foreseeable future, we must adopt security standards that will live comfortably alongside our new routines. Put another way, there is no end to this road we are on; we are now in a state of



automated. Even at massive scale, any device that connects to the corporate network is assessed and logged, from home PCs to cloud services, software containers and IoT devices. If it reads, creates, or updates data, you will know about it. Welcome to a world in which real-time tracking and vulnerability scanning are standard.

Sound asset management allows you to patch more easily. Vulnerabilities are a fact of life in technology ecosystems. Dealing with them sensibly is one of the most essential jobs of today's IT teams. But methodically going through every app and manually applying every available fix is impractical and counterproductive.

“NEW BEST PRACTICES ARE REQUIRED TO ENSURE EVERYONE CAN WORK WHEREVER, WHENEVER, AND HOWEVER THEY NEED TO.”

this properly will not only lead to greater operational efficiency within the security function itself. It will also make it easier to feed line of business with clear reporting on how protection measures are applied across the entire business... and how effective they are.

The unique consequences of the global COVID-19 pandemic have forced some hard decisions upon organisations and their CISOs. The economic malady outside the walls will force security teams to justify their budgets and even their very existence. Cloud security spending may be on the

perpetual adaptability. While the region's workplaces are changing, some other realities are not. Attackers are still out to get us; regulators still expect compliance; and customers still expect privacy and safe commerce.

So, while we chase a galloping horizon, we should be vigilant. Transparency regarding performance, regular reporting, benchmarks, metrics and all the tools of accountability must be brought to bear on those responsible for delivering safe environments. Nobody ever said implementing best practices was easy. But the rewards are significant, and the alternative is unthinkable. 🧑🏻‍💻

RANSOMWARE: WHAT IS YOUR DATA WORTH?

MARK NUTT, SENIOR VICE PRESIDENT, EMEA,
VERITAS TECHNOLOGIES, WEIGHS IN ON THE
AGE-OLD IT SECURITY QUESTION – SHOULD
YOU OR SHOULD YOU NOT PAY RANSOMWARE?

Ransomware attackers have been turning their gaze away from ordinary consumers as companies and enterprises offer more fertile hunting grounds, and the promise of much larger rewards than the average home user. For many hackers, attacking the little guy is no longer worth the effort.

However, this doesn't mean our personal data is safe and sound. We all have data that is precious to us but looked after by somebody else. Dealing with almost any business today involves trusting them with some kind of data – whether it's our medical records, financial information, shopping habits, family photos, or even our dating profiles.

If the data you share with a company is stolen or encrypted during a ransomware attack, retrieving it can be difficult. But should the company pay to have it returned? And what can you do as an individual to help keep your data safe in the first place?

To pay or not to pay?

Data can say more about you than any simple financial transaction. So, when your data falls into the wrong hands, the impact can be devastating. If a criminal steals money from you online, you can often be reimbursed by your bank, insurer or issuer; but if a criminal

steals your data, they can hold power over you long after the event.

Some data, such as family photos or academic work, can be irreplaceable on a personal level, but many types of data loss can be damaging. Imagine, for example, trying to get a new job without being able to prove your qualifications.





Think about the cost of x-rays to recreate your dental records. Or consider simply not being able to qualify for the no-claims bonus on your car insurance. Any of these things could happen as the consequence of your data being stolen in a ransomware attack on one of the companies you currently do business with. So, shouldn't the company pay to fix things?

The case for a company paying the ransom for your data may appear strong but, sadly, the hope of regaining your data this way is often wishful thinking. Even if the ransom is paid, there's no guarantee the attacker will return your information. Many hackers couldn't give

it back even if they wanted to, since they lack the technical capabilities to reverse the process they started. Little wonder then that 20 percent of paying victims don't even have their stolen data returned.

And consumers rarely want the businesses they trust to be complicit in allowing crime to pay. Veritas research shows that under a quarter (23 percent) of consumers think that businesses should negotiate with cybercriminals. Similarly, just 27 percent think governments should engage with the attackers. In the majority of cases, prevention is far better than the cure. Customers say they expect the organisations that they buy from to have strong ransomware defences and a comprehensive data backup policy.

**"ALL TOO OFTEN,
A RANSOMWARE
ATTACKER CAN
BRING ITS VICTIMS
TO A PLACE WHERE IT
FEELS LIKE THERE'S
NO RIGHT DECISION."**

Staying safe, without surrendering

All too often, a ransomware attacker can bring its victims to a place where it feels like there's no right decision. If the data can't be restored another way, they must either pay the ransom and invite repeated attacks in the future, or they lose their data forever. Neither choice is a victory. When faced with an impossible decision, all anyone can do is work out how they got there in the first place and ensure it never happens again.

Ransomware attacks on ordinary consumers are rarer now, but they still happen. To avoid being caught out, be diligent when it comes to what emails you open and which links you click, and ensure you're using up-to-date antivirus software. But you should always work on the assumption that a new virus or scam could sneak past your best defences. And, here, preparation is the key to success. Backing up your files is easy and, just to be safe, you should be saving multiple copies in different locations, such as external drives or in the Cloud. That way, if a hacker comes after your data, and successfully encrypts it, you don't need to pay – you can simply restore another copy.

But, how do you protect the personal data that isn't on your own computer? How do you defend the data that businesses hold on you?

The best way to do this is to make an informed and responsible decision over who you purchase from. Before engaging with a business that's going to hold records on you, read its data policy carefully and check up on their history. Under GDPR, businesses are obliged to defend the data of their customers, but the enforcement leaves a lot of freedom for businesses to comply as they see fit, and not all invest the same resources in data protection.

If a business has a history of data breaches, or fails to mention the steps they take to protect customer information or back up their data, this should throw up a red flag. Just as you would never want to fly with a carrier that has a poor track record for safety, you shouldn't be trusting your information to a business that has a poor track record for security. You're not powerless to protect your data online; your choice of whom you do business with can make all the difference. 🗝

SIMPLIFIED CONNECTIONS

DAN KLIMKE, DIRECTOR OF MARKETING, NETALLY, ON HOW THE COMPANY IS PROVIDING TOOLS TO SIMPLIFY NETWORK TESTING AND DELIVER INCREASED VISIBILITY ACROSS WIRED AND WIRELESS NETWORKS.

Can you please give us a brief background about NetAlly?

NetAlly has started as an independent company in 2019. We were formerly a business unit of NETSCOUT and previously part of Fluke Networks.

However, we have been in the industry since 1993 when we created the industry's first handheld network analyser in 1993, which was designed for IBM Token-ring networks but soon included ethernet.

In 2015, the communications division that we were a part of under Fluke Networks was purchased by NetScout. Then after four years, we were bought out by a private owner and now we're running as an independent company. We are focused on developing handheld network testing devices and network analysis software for WiFi. Our aim is to simplify the complexities of network testing and provide instant visibility for efficient problem resolution across wired and wireless networks.

As the world continues to adapt to the ongoing COVID-19 pandemic, enterprises are grappling with having to manage fragmented networks as they adopt hybrid working models. How can they ensure network visibility amid this new normal?

There are two dynamics that we have to look at. One is the work-from-home dynamic and the other is IT teams can manage remote sites when travel is probably not possible. So, thinking about the workers from home, everyone is relying on their local service providers and their home networks to deliver connectivity to cloud-based and corporate resources. For users in that circumstance, home networks provide adequate bandwidth for their needs but in some cases, there may be issues with their home wireless network or their internet service provider. In some instances, we would ship our handheld devices to our customers to get detailed visibility of that worker's home network. This brings me to point number two, troubleshooting networks remotely has always been an issue for network

operations and for enterprise IT, whether you have staff onsite or not.

In many cases, organisations may have IT support staff on-site but perhaps they're not skilled enough to manage and solve the kinds of problems that can occur in their local network. So, that has frequently meant that some centralised experts have to travel to those remote sites to do some troubleshooting and analysis.

We've tried to solve that problem through tools that enable remote collaboration. So, rather than just being a standalone piece of test equipment, our tools can be connected to the cloud. We have a cloud service called Link-Live, which is a cloud-based platform for collecting, managing, and analysing test results and site data uploaded from NetAlly network testing tools. This allows network engineers can take control of a test unit and remotely troubleshoot any network issues. So, despite being confined to our home offices there are still plenty of ways to get the right kind of visibility needed to solve problems for remote workers.

“OUR AIM IS TO SIMPLIFY THE COMPLEXITIES OF NETWORK TESTING AND PROVIDE INSTANT VISIBILITY FOR EFFICIENT PROBLEM RESOLUTION ACROSS WIRED AND WIRELESS NETWORKS.”

What are the primary WiFi deployment mishaps that IT teams commit?

The dynamics are different depending on the size of the organization and the size of the site. For most larger commercial enterprises and government agencies, they typically rely on systems integrators for an initial design and installation. Hopefully, those integrators use the right kind of design, installation and validation tools. However, sometimes even if they had a good starting point, there will still be issues such as network performance, visibility gaps or lack of coverage, which are all very common. Among the key mistakes that IT teams commit is simply adding more capacity and access points, this results in over-provisioned networks, making them less efficient.

How can enterprises make the process of Wi-Fi deployment and troubleshooting simpler?

We've come up with a new way to survey WiFi networks. At NetAlly, we have products in our portfolio that are aimed at ensuring effective wireless network planning, installation and validation.



Our AirMagnet software product line has been one of the leading products in the industry for that purpose. It's an effective analysis and monitoring software tool for mobile monitoring, auditing and troubleshooting enterprise WiFi networks. AirMagnet helps IT staff quickly solve end-user issues while automatically detecting WiFi signal strength, security threats and wireless network vulnerabilities.

We also have AirMapper, which allows IT teams to quickly and easily gather location-based Wi-Fi measurements and create visual heat maps of key performance metrics in the Link-Live Cloud Service. This is ideal for quick site surveys for new deployments, validating changes, and fast performance

verification, NetAlly is the first to provide a complete site survey and wired/wireless analysis solution in a handheld instrument.

What can we expect from NetAlly in the coming months?

Being an independent company, we are focused on chartering our own course with respect to our R&D. Our engineers have been phenomenally productive over the last year with the pace of our product innovations. We have an aggressive roadmap for 2021. We will be developing new features for our Link-Live Cloud Service and introduce new offerings. We will continue to be in-the-know about the latest technologies in the market to keep up with the needs of our customers. 📌

KEY BENEFITS OF SECURE SD-WAN FOR ENTERPRISE CUSTOMERS

BY **JON BOVE**, VP OF CHANNEL SALES AT FORTINET



Enterprise customers have long relied on wide-area networks (WANs) to support multi-locale business communications. But as the adoption of cloud-based services, SaaS applications, and BYOD increases, traditional WAN performance has struggled to keep up with their rising bandwidth requirements. Meanwhile, today's digital businesses require not just flexibility but also meshed interoperability between users, applications, and devices, something that most static WANs cannot provide.

It is factors such as these that have led organisations to adopt software-defined wide-area network (SD-WAN) solutions that can adapt to the new networking requirements brought on by digital transformation. Offering more agility, responsiveness, and cost-effectiveness for enterprise customers SD-WAN improves application performance for highly-trafficked networks.

SD-WAN is a cost-effective alternative to WAN infrastructure that improves speed and branch uptime through public network broadband. That said, when it comes to securing SD-WAN, for example, many IT leaders struggle with the cost and complexity associated with developing, deploying, and maintaining an overlay solution. The reason this happens is because most SD-WAN vendors provide little to no security as part of their solution. As a result, customers have to apply security as an afterthought.

Single appliances, where all networking, connectivity, and security functionality are fully integrated into a single, coherent system, are always going to be much more efficient than disparate solutions that work to serve individual purposes. This means that security must be deployed not as an isolated overlay but as an integrated feature that makes it easy to protect

constantly changing network functions like bandwidth sharing and link error corrections. At the same time, an integrated approach also ensures that performance is not compromised even when it comes to processor-intensive activities such as deep inspection of complex VPN connection overlays.

Deploying a smartly-integrated solution that addresses both customer networking and security challenges help organisations realise a range of benefits, including being cost-effective, reduced complexity, and centralised management capabilities that span the entire SD-WAN deployment. Additionally businesses can benefit from improvements in bandwidth for high- application performance and enjoy enterprise-grade security with consolidated networking functionality.

Businesses can accomplish much more with Secure SD-WAN capabilities than with a traditional SD-WAN solution. By leveraging an integrated Secure SD-WAN solution, enterprise customers can easily manage internet connectivity and performance while simultaneously eliminating the costs associated with implementing separate security solutions as an overlay for an unsecured SD-WAN.

“TODAY’S DIGITAL BUSINESSES REQUIRE NOT JUST FLEXIBILITY BUT ALSO MESHED INTEROPERABILITY BETWEEN USERS, APPLICATIONS, AND DEVICES, SOMETHING THAT MOST STATIC WANs CANNOT PROVIDE.”



AVEVA

Edge to Enterprise

A new approach to Industrial and
Infrastructure Monitoring & Control

 aveva.com

 [@avevagroup](https://twitter.com/avevagroup)

 linkedin.com/company/aveva

Building a Fully Connected,
Intelligent World



HUAWEI CLOUD

Grow with Intelligence



Know More