

cnme

computer news middle east

WHERE TECHNOLOGY MEANS BUSINESS

ISSUE 344

NOVEMBER 2020

TAHAWULTECH.COM

MANAGING RISK

BHARAT RAIGANGAR, WIPRO, AND SANCHU SANKAR, MICROSOFT HIGHLIGHT HOW ENTERPRISES NEED TO ADOPT A 'CLOUD-NATIVE MINDSET TO SECURITY' IN THE CURRENT DIGITAL ECONOMY.



CITRIX'S REGIONAL
DIRECTOR MENA

CYBEREASON'S
CSO

VERITAS'S
SVP, EMEA

CPI MEDIA GROUP

CPIMEDIAGROUP.COM

PUBLICATION LICENSED BY
DUBAI PRODUCTION CITY, DCCA

 tahawultech.com



Securing a futuristic world

SecureTech Crosses Another Milestone

Achieves Huawei's highest tier solutions partner: Value Added Partner



Our events



Our online platforms



Our social media



facebook.com/tahawultech



twitter.com/tahawultech



linkedin.com/in/tahawultech



Talk to us:
E-mail:
mark.forker@cpimediagroup.com



There is no longer
the question of if
when it comes to
cloud migration,
instead the
question
is when."

HEAD IS IN THE CLOUDS

Over the last number of months, the sheer volume, scale and speed at which digital transformation has been rolled out across the entire Middle East region has been staggering.

However, there has also been an exponential growth in cloud transformation as more and more enterprises migrate to a hybrid consumption-based cloud model.

There is no longer the question of if when it comes to cloud migration, instead the question is when.

Cloud is key and it's going to continue to dominate the IT ecosystem in 2021, and the central theme of our front cover story in November's edition of CNME revolves around the modernisation of Security Operations Center – and how a cloud-native approach is required when it comes to security in this on-demand data-driven digital economy.

We spoke to Bharat Raigangar from Wipro and Sanchu Sankar from Microsoft to learn more about the collaboration between the two entities, their views on SOC's, the evolving demands of consumers and the unique capabilities of Microsoft Azure Sentinel.

In this month's magazine I also got the opportunity to speak to Taj El-Khayat, Regional Director, MENA region at Citrix, to find out why the company has decided to undergo a corporate rebranding, how its solutions are empowering employees and what the future of the workplace will look like.

Huawei are a global leader in terms of innovation in the ICT sector and I also managed to secure an exclusive interview with Nadim Abdulrahim, Global Government Industry Expert, Huawei Enterprise Business Group, Middle East, to learn how city administrators are coping with new trends emerging from the COVID-19 pandemic, and how cloud is key in fueling cities of the future.

We continued our trend of virtual webinars in November – and featured in this month's edition of the magazine are post-event coverage of interactive roundtable discussions with A10 Networks, BeyondTrust and Cybereason.

We have also got a series of superb op-eds from prominent technology thought leaders from companies such as Ericsson, AppDynamics and JP Morgan.

Mark Forker
Editor



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

GITEX.COM #GITEX2020

Some of our 2020 Exhibitors



هيئة الطرق والمواصلات
ROADS & TRANSPORT AUTHORITY





6 News

CNME rounds up the biggest regional and global developments in enterprise technology, which includes the launch of a new data analysis lab by STC, which has been designed to foster AI innovation in Saudi Arabia, Accenture and ServiceNow have teamed up to form a new business group to drive digital transformation – and Riverbed appoints a new CIO.

18 Citrix

Taj El-Khayat, Regional Director, MENA region at Citrix, explains why the IT leader has undergone a comprehensive corporate rebranding, and highlights how Citrix are elevating their employees to have a higher purpose.

22 Huawei

Nadim Abdulrahim, Global Government Industry Expert, Huawei Enterprise Business Group, Middle

East, tells us how city administrators coped with the COVID-19 pandemic.

32 JP Morgan

David Stubbs, Head of Market Strategy & Advice at JP Morgan Private Bank, takes an intrinsic look at the impact digital transformation has had on the already burgeoning FinTech sector.

42 Ericsson

Said Zantout, Head of Solution Area OSS, Core and Cloud at Ericsson Middle East and Africa, outlines the capabilities eSIM can have for consumers in our digitally driven economy.

48 AppDynamics

David Noël, regional vice president, Southern Europe, Middle East & Africa at AppDynamics, explains the importance of end-to-end network visibility in order to deliver a modern digital experience.

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 9138

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

EDITORIAL
Editor
Mark Forker
mark.forker@cpimediagroup.com
+971 4440 9153

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

PRODUCTION AND DESIGN
Senior Designer
Analou Balbero
analou.balbero@cpimediagroup.com
+971 4 375 5680

DIGITAL SERVICES
Web Developer
Jefferson de Joya
Abbas Madh

webmaster@cpimediagroup.com
+971 4 440 9100

Publication licensed by
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.

stc launches data analysis lab to accelerate AI innovation in Saudi Arabia

stc group CEO Nasser bin Suleiman

AI-Nasser called on large companies to adopt transformative plans to promote innovation through artificial intelligence (AI), and to develop solutions that aim to support the growth of sectors while reducing the costs in each of them.

During his participation at the recent Global Summit on Artificial Intelligence, organised virtually by the Saudi Data and Artificial Intelligence Authority (SDAIA), AI-Nasser pointed out that stc relied on various AI technologies that



serve customers and the group in order to improve efficiency and create better experiences for customers and thus contribute to increasing revenues and reducing costs.

In the same context, stc announced the launch of an Advanced Cloud Based

Data Analysis Laboratory through which big data and predictive analysis as well as AI innovation can be analysed by providing an integrated structure that supports the use of advanced methods and techniques that support open sources.

Ripple chooses DIFC for regional headquarters

6



Enterprise blockchain solution for

global payments, Ripple, has announced that it has chosen Dubai International Financial Centre (DIFC) as the location of its Middle East headquarters.

According to Ripple and DIFC their visions are aligned to shape the future of finance.

Established in 2012, Ripple builds financial solutions and services to move money at the same speed and standard that information moves today. By joining Ripple's global financial network,

RippleNet, customers can process their payments instantly, reliably, cost-effectively and with end-to-end visibility anywhere in the world. Hundreds of financial institutions already use RippleNet in more than 45 countries, making it one of the leading providers of blockchain for payments.

Arif Amiri, Chief Executive Officer of DIFC Authority, said, "Leveraging DIFC's world class platform, laws and regulations, our FinTech firms are able to work with other DIFC's clients, who form part of the region's largest financial ecosystem, to contribute to the development of the global, regional and local finance industry. During this post-pandemic recovery period, we recognise how digital agendas are being prioritised. Ripple and the other 230+ FinTech related companies in the Centre are key to driving the future of finance."

"Ripple is one of the most exciting client additions to DIFC this year.

They are well regarded globally for innovation in the finance industry and therefore is a perfect partner and client for DIFC, given our vision to drive the future of finance. Together, we will advance the use of blockchain in Dubai, UAE and the region, and accelerate the Emirates Blockchain Strategy 2021."

"Together, we will advance the use of blockchain in Dubai, UAE and the region, and accelerate the Emirates Blockchain Strategy 2021."

Accenture, ServiceNow bolster support for digital transformation

Accenture and ServiceNow have formed a new business group to help private and public sector clients accelerate their digital transformation and better address today's dynamic operational challenges.

In the COVID-19 era, organisations are under more pressure than ever to innovate faster, reduce costs, enhance productivity, and meet their customers' needs. The Accenture ServiceNow Business Group will help organisations rapidly evolve organisational processes and unlock the full value of technology investments by adopting digital workflows that deliver modern, personalised customer and employee experiences.

ServiceNow CEO Bill McDermott said, "Leaders in every organisation know



Bill McDermott, CEO, ServiceNow

that their 20th century technologies are too slow, too siloed, too stuck in the status quo to meet the dynamic digital demands of employees and customers today. Speed, agility, and resilience are what's needed now. Our ServiceNow and Accenture partnership brings together world-class teams, expertise, and our modern workflow platform to accelerate every organisation's digital transformation. The Accenture ServiceNow Business Group will help every organisation become a 21st century digital business."

Smart tech boosts UAE's healthcare market to \$21 billion

Smart healthcare technology innovations to combat the COVID-19 coronavirus and improve people's daily lives are at the centre of the UAE's healthcare spend topping \$21 billion by 2021, industry experts have announced.

The UAE government continues to increase its healthcare spend –

"The UAE's healthcare spend is set to top \$21 billion by 2021, according to the United States – UAE Business Council."

especially in supporting healthcare technology innovations that can help to manage lifestyle diseases and coronavirus. As a result, the UAE's healthcare spend is set to top \$21 billion by 2021, according to the United States – UAE Business Council.

"Healthcare technology innovations are the foundation of the UAE's record-high healthcare spend," said Andrew Calthorpe, CEO, at Condo Protego. "Across the UAE, healthcare providers are leveraging technology to help counter the coronavirus now, and to deliver new levels of patient-centric healthcare in the future."

Healthcare providers should take a 4-step process in their digital transformation: modernising IT infrastructure, maintaining 24/7

Saudi Arabia's largest shopping mall operator redefines CX with Oracle

Arabian Centres Company, the largest owner, developer and operator of contemporary lifestyle malls in Saudi Arabia has announced that it has implemented Oracle Fusion Cloud Applications. cloud future business

The deployment, according to the organisation, is part of a major core business process transformation.

The initiative will help Arabian Centres Company enhance business efficiency, deliver unique omni channel customer experience, introduce innovative services and prepare a digital ready workforce.

"Customer expectations and priorities for a retail experience have changed dramatically over the past few months, and while our 21 lifestyle malls across 11 cities can cater to more than 100 million visitors, we now need to introduce a more innovative omni channel retail experience for our vast customer base", said Faisal Aljedaie, Chief Executive Officer, Arabian Centres Company. "With Oracle Cloud Applications, we will be able to swiftly adapt business models based on latest customer behaviour data, reduce costs, introduce innovative experiences and sharpen forecasts."

cloud access, launching mobile apps, and enhancing cybersecurity, argues Condo Protego, the leading UAE-based IT infrastructure and information management consultancy and solutions provider.

Dubai-backed Virgin Hyperloop completes test drive with human passengers

Virgin Hyperloop has made history

after successfully completing the world's first hyperloop test drive with human passengers.

Josh Giegel, Co-Founder and Chief Technology Officer, and Sara Luchian, Director of Passenger Experience, were the first people in the world to ride on this new form of transportation. The test took place at Virgin Hyperloop's 500-meter DevLoop test site in Las Vegas, Nevada, where the company has previously run over 400 un-occupied tests.

Dubai-based leading global provider of smart logistics solutions, DP World, has made a multi-million dollar investment for the research and development of hyperloop technology, leading to today's milestone.

Sultan Ahmed Bin Sulayem, Chairman of Virgin Hyperloop and Group Chairman and CEO of DP World, watched this passenger testing first-hand in Las Vegas, Nevada.

"I had the true pleasure of seeing history made before my very eyes – to witness the first new mode of mass transportation in over 100 years come



to life," said Sultan Ahmed Bin Sulayem, Chairman of Virgin Hyperloop and Group Chairman and CEO of DP World. "I have always had tremendous faith in the team at Virgin Hyperloop to transform this technology into a safe system, and today we have done that. We are one step closer to ushering in a new era of ultra-fast, sustainable movement of people and goods."

"I had the true pleasure of seeing history made before my very eyes – to witness the first new mode of mass transportation in over 100 years come to life."

He added, "DP World and Dubai are at the forefront of technological innovation in the transport and logistics industry. The world has been changing quickly and we wanted to be involved in the potential this mode of mass transportation presents, to connect markets and economies, keep trade flowing and help build the global economy's next phase to accelerate growth."

Riverbed names Sekhar Kancherlapalli as CIO

Riverbed has announced the

appointment and promotion of Sekhar Kancherlapalli to Chief Information Officer (CIO).

In his new and expanded role, Kancherlapalli will oversee all IT functions and operations, and will be focused on leading and furthering Riverbed's cloud and digital initiatives. Prior to joining Riverbed as a Chief Architect, Kancherlapalli held senior cloud and enterprise architecture roles at Oracle, Liberty Mutual Insurance and Fidelity. He will join Riverbed's Executive

Leadership Team and will report to President and CEO, Rich McBee.

"Driving a digital transformation strategy is at the core of my expertise and Riverbed's digital and cloud journey is fundamental to the company's overall success," said Sekhar Kancherlapalli, CIO of Riverbed. "Additionally, Riverbed's own solutions play a crucial role for our IT team and business, enabling us to maximise performance and visibility across applications and networks, regardless of where users reside. I



Sekhar Kancherlapalli, CIO, Riverbed

look forward to the IT organisation continuing to be in the forefront and leading with the business."

CNS Middle East, RackWare offer customers seamless migration to Oracle Cloud



CNS, a trusted digital innovation and enterprise technology partner operating in the UAE, Oman, Kuwait and broader Gulf region is amongst one of the first Oracle partners in the region to enable migration to Oracle's recently opened

Dubai Cloud region. To augment this capability, CNS has partnered with RackWare to offer an added-value service to Oracle customers in the Gulf region that will help their seamless migration to Oracle Cloud.

RackWare is a leading provider of Hybrid Cloud Management and a member of Oracle PartnerNetwork (OPN). The RMM Cloud Management Platform enables cloud migration, image mobility, disaster recovery, backup, intelligent provisioning, auto-scaling, and cloud governance that harnesses the benefits of Oracle Cloud Infrastructure. Taking advantage of their superior market access in the region, CNS Middle East will execute the platform's implementation with their existing specialized local IT capabilities and expertise.

As one of the top Tier 1 Oracle partners in the region, CNS can fully apply Oracle Cloud's technological advantages to their client's business needs. "Integrating RackWare capabilities into our portfolio of technology solutions will allow us to bridge the gap between customers' current cloud adoption and requirements with Oracle Cloud Infrastructure, allowing us to improve and optimize our clients' complete infrastructure," said Hatem Hariri, Managing Director of CNS. "As a managed services provider, not only does this make our jobs easier, but our clients also get the same updated functions of Oracle Cloud Infrastructure with the familiarity of their legacy solutions."

9

Finesse, Capillary Technologies to offer omnichannel customer loyalty solutions

Finesse has joined hands with Capillary Technologies, an award-winning cloud-based Loyalty platform, Customer Relationship Management (CRM) and Omnichannel Customer Engagement solution for retail and consumer brands.

Capillary Technologies will power Finesse's Clients with an engagement-based loyalty platform. The platform increases brand recall and repeat sales by incentivising customers in real time for their transactional and non-transactional (likes, shares, reviews, and more) brand interactions.

With this alliance, Clients will be able

to harness the combined power of the regional presence and strong delivery capabilities of Finesse with the world-class products of Capillary. Finesse and Capillary will mutually align go-to-market initiatives to deliver superlative value to customers.

Eljo J P, Director & Chief Business Officer, Finesse Global, said, "Capillary Technologies enables us to offer full-stack personalised customer engagement, omnichannel loyalty marketing and consumer analytics solutions that help our Clients understand their consumers at a granular level. Today, with



Bill McDermott, CEO, ServiceNow

global customers using both digital and physical channels, Capillary will help our clients improve marketing effectiveness and ROI by enabling a unified connected customer engagement strategy."



Sam Curry
CSO at Cybereason

MAKING SENSE OF THE CHAOS

CNME Editor Mark Forker moderated a virtual roundtable with **Sam Curry**, CSO at Cybereason, to learn how a SOC (Security Operations Centre) can help bolster and protect government entities and large enterprises from cyber threats and attacks.

Curry is one of the most decorated and distinguished cybersecurity experts in the IT ecosystem and has over 25 years of experience in the sector.

It has been well documented over the last number of years that the sophistication of cyberattacks has increased and its threats come in many different forms and continues to evolve, and that has also been further supplemented by the ongoing COVID-19 pandemic.

The virtual roundtable was entitled 'Defending Chaos and Corporate Risk' and the charismatic American helped to make the session extremely engaging in the way he conducted and delivered his presentation.

Before he began his presentation, Curry provided some background on Cybereason in terms of its mission since its inception and outlined the role their playing in the IT security industry.

"Cybereason as a company was founded with a mission. We believe in what we call the connected world and we believe in what digital transformation can do for the human experience, what it can do for governments, enterprises and us as individuals. However, we believe that it is fundamentally at risk due to hacking and cyber threats, so our mission as a company is to reverse the hacker advantage," said Curry.

Curry stressed how it was important it was to understand the differences between two types of risk in the security environment. He highlighted how over the years

many C-level executives and board members have said to him when will we solve the security problem and find one solution that simply takes care of security?

According to Curry, this didn't sit right with him, citing the reason that is it is a different kind of risk to the normal kind of risks managed in companies.

"First order chaos is natural systems, a hurricane or a tropical storm is a threat in a first order chaos system of meteorology. COVID-19 is a first order chaos risk in the biological system. Second order chaos are systems that can intelligently adapt. If COVID-19 was a second order chaos risk would say to itself I'm going through an airport I should lower my hosts body temperature to make it past this hurdle, but it doesn't do that, because it isn't intelligent enough to adapt, but that's precisely the risk we face in security," said Curry.

Curry kicked off his presentation by posing the



We believe in what we call the connected world, and we believe in what digital transformation can do for the human experience."

question of what was the mission of security? He then proceeded to outline what he felt was the biggest issue currently afflicting the entire security landscape.

“My biggest concern in the security industry is the fact that most security departments don’t align with their businesses very well. It is a major source of concern. If you ask a CFO what the job of sales is, they will say, that’s easy they bring me the money. If you ask them what the job of marketing is, they’ll say that is also easy, they help sales make money. But when you ask them what the job of security is, they’ll give you a blank look. They will say they always talk about risk, but they don’t understand the other forms of risk in our business, but essentially the main job of security ultimately is to stop threats faster and more completely, and in order to do that effectively it needs to be aligned to the business,” said Curry.

Curry stated that he believed that IT security is not the same as cybersecurity, although he admitted that this may be considered a controversial opinion by other industry peers.

“There are key use cases that demonstrate the nuanced differences between IT security and cybersecurity. But what do I put in each bucket? Well in the IT security bucket I put things like reporting, vulnerability and patch management, the deployment of a reference architecture, and by that I’m

referring to simple preventative tools. The use cases I put in cyber are very clear. We need to build tools and processes that bring the mark 1 human intelligence to bear in defending against human intelligence in offense. How do we make that more effective? I believe that AI in AI should stand for assisted intelligence, rather than artificial intelligence, because too often we find security companies and services companies say AI and wave their hands, and they’re trying to convince you is that they’ve got some incredible robotic intelligence that can just

do this job. There is intelligence in security, but it is carbon-based not silicone-based, and it is our job to identify these use cases,” said Curry.

Curry then illustrated the importance of the evolution of the cyber machine, stressing how the security industry needs to do better or run the risk of losing the race.

“The evolution of the cyber machine is essentially how we get better at doing the job, and I don’t mean incrementally, because it’s a race. It’s an asymmetric race, and the kid on the other side is not using





the same tools, he may be using the same base algorithms and mathematics, but the application is radically different. I don't believe it's good enough to simply say AI and we're done, instead we need to think how to we make these people as effective as possible with the result that we want. When we do find AI that can help us with this job. I do believe it will be groundbreaking. I believe that Machine Learning has delivered for us usable tools to make assisted intelligence as oppose to artificial intelligence practical," said Curry.

Curry then examined the key use cases required to enhance prevention, resilience and antifragility within a government entity or large multinational enterprise.

"I really do want to emphasize that when we do IT



I believe that the A in AI should stand for assisted intelligence, rather than artificial intelligence."

security and cyber, we should always be thinking about we can get closer to immediate prevention and becoming more resilient and demonstrating antifragility. We believe that once you have defined your processes you can tighten them and tune them and remove waste from them. One of the problems we have in the security domain is that we have advanced by being the smartest people technically from a security perspective throughout our careers. However, what we very often don't realise is that suddenly when we jump and become managers or directors, we have to go outside and get a whole body of knowledge that is sometimes absent in our companies around the management of people and processes," said Curry.

He added that if you agreed with his hypothesis that cyber is in fact a machine, whose job is to stop things more completely and sooner, and is aligned to the business, then this is fundamentally understandable.

"The biggest problem in security, which I alluded to earlier is we're not aligned to the business. I was asked by a journalist when will the cyber problem finally be done? I said I don't think it can be, but it can be brought to acceptable levels. The job isn't to try and change human nature, in the long-term we will let the scientists figure out how to defeat cyberthreats completely, but in the meantime, it can be brought to acceptable levels," concluded Curry. **crme**

VEEAM

PREDICTING THE FUTURE

Danny Allan, CTO and SVP Product Strategy, at Veeam, gives us his predictions on what technologies and topics will fuel innovation and shape conversations in the IT ecosystem in 2021.



Danny Allan
CTO and SVP Product Strategy, at Veeam

Developers will have more say in technology direction and data strategy of companies:

We will see an aggressive “shift to the left” across all industries, where CIO’s will depend more on their development teams to guide the technical direction of the company.

Historically, development teams have taken a top-down approach to move their data to the cloud, but – as have many things in the world – this changed with the pandemic with the reinforcement of cloud-based environments.

In 2021, we’ll see DevOps teams continuing to have far more say in the data strategy process, and as a result we’ll see a greater increase in the mobility of workloads, correlating with an increase in cloud data management techniques.

A greater focus on protecting and managing work collaboration platform data in the cloud:

Distributed workforces were already on an upward trajectory but have been completely kicked into overdrive with the COVID-19 pandemic.

With many companies extending work-at-home opportunities through mid-next year, reliance on cloud-based collaboration platforms such as Microsoft Teams and Slack, will only increase. This means even more teams will be looking to harness the power of the cloud

to store an influx of data from collaboration platforms.

In 2021, this will create more focus, awareness and need for data protection and management for collaboration software.

With the decline of hardware, software-defined models will become more prominent:

Appliances will diminish in their attractive as we shift towards software-defined models. 10 years ago, appliances where these shiny new toys that everyone wanted to get their hands on, however they have not had the staying power we predicted they would.

In fact, we've seen a shift towards backup-as-a-service and away from appliances. Remote work in the pandemic had a real impact on how we dealt with hardware in 2020 that will continue into 2021 as software-defined models take center stage.

Machine learning will become democratised in the cloud around data:

Already, we are seeing organisations recognise the unlimited opportunities available to them through data they have already collected. Data re-use will be a big trend we see organisations shifting to 2021, with many leveraging the power of machine learning to help them do this.

This is still in the emerging stages; however, its adoption will increase as organisations recognise how it



Appliances will diminish in their attractive as we shift towards software-defined models.”

can help them analyse and re-use data that they already have. By leveraging machine learning in the cloud, organisations will ultimately become smarter.

Compliance regulation fines won't see an uptick – they're going to continue trending down:

Data privacy and privacy regulations will continue to gain traction in 2021. In particular, I predict we will see the first proposed federal regulations around privacy in the New Year. However, compliance fines will continue on the downward trend we saw in 2020.

We saw a massive jump in compliance fines in 2019, which solidified how seriously GDPR, CCPA and others needed to be taken. Now that this attention has been received and the awareness is there, the shift will be more towards more consistency of privacy regulations at the federal level.

IT spending will rebound after 2020 – security and hardware will be at the top of the list.

Despite the economic turbulence brought on by the pandemic

in 2020, we'll see a five to 10 percent increase in general IT spend in the New Year.

Allocations will likely focus most on security, general system modernisations (backup, applications, cloud migrations, etc.) and refreshing hardware. In addition, organisations will take a look at what was on “hold” in 2020 to address IT spend that happens on an annual recurring basis.

For example, hardware should be refreshed every three years, and if the pandemic halted an organisation's attention to hardware, it's fair to say that will make its way to the top of the list in 2021.

Developers will have more say in technology direction and data strategy of companies

We will see an aggressive “shift to the left” across all industries, where CIO's will depend more on their development teams to guide the technical direction of the company.

Historically, development teams have taken a top-down approach to move their data to the cloud, but – as have many things in the world – this changed with the pandemic with the reinforcement of cloud-based environments.

In 2021, we'll see DevOps teams continuing to have far more say in the data strategy process, and as a result we'll see a greater increase in the mobility of workloads, correlating with an increase in cloud data management techniques. **CNME**

HPE ARUBA

PROTECTING EDUCATION

Jacob Chacko, Regional Business Head, Middle East, Saudi & South Africa at HPE Aruba, has appealed to the education sector in the Gulf region to start taking cybersecurity seriously in an exclusive op-ed for November's edition of CNME.



Jacob Chacko
Regional Business Head, Middle East,
Saudi & South Africa at HPE Aruba

There has never been a greater need to connect students, classrooms, and buildings. Enrolment of students (who are always more tech savvy and more expectant than the year that preceded them) continues to rise, and the benefits of technology – better grades and greater staff well-being – are necessary if schools are to maintain high levels of performance during the challenging time of digital transformation.

What's key, however, is that cyber security is taken seriously. Not in a way that restrains a school's ambitions to innovate, but so that technology is controlled and managed with caution to protect the students.

This will become increasingly important as schools and universities expand deployment of digital, collaborative and immersive learning environments across new and modernised buildings and campuses.

Here's a closer look at some of the advances many schools are making today, and the security measures that can, and should, be taking to protect their data and reputation.

The changing face of education:

There are exciting times ahead for the education industry. Typically, this sector is one of the last to make extensive change, but thanks to the ambitions of teachers keen to engage better with students, the classroom of yesteryear is starting to transform. In many schools, where once Wi-Fi was limited to a handful of

classrooms, now any room can be used as an IT suite.

New tech such as eLockers are being trialled as a way of empowering students and encouraging self-paced learning. And, rather than deter the use of personal devices, they are becoming increasingly more embedded in the educational toolset.

And so, by enabling a more digital workplace, staff will be freed up to make faster decisions and engage students whose learning styles vary. Already we're seeing education employees reap the rewards of technology. In Aruba's recent study of more than 1,000 employees, almost three quarters (74%) said they could accomplish more throughout the day and had the opportunity to develop new skills (74%).

However, as the smarter classroom gradually becomes a reality, so the question of security – and how it is managed – must be addressed.

Keeping security in check as progress is made

Worryingly, just under half (49%) of teachers admit they rarely (if ever) think about cybersecurity, despite 91% acknowledging its importance. In addition, more than three-quarters (76%) believe there is room for improvement in the way connected tech is managed.

This is a challenge for institutions. Schools, colleges and universities alike share the same priority: providing the best possible education to cater to students whose expectations are growing exponentially.

To connect with them in

a meaningful way requires reliable, optimised, and personalised learning experiences. But an influx of Internet of Things (IoT) devices and a cohort that aren't all trained in security best practices, puts networks at risk of intrusion. And, more seriously, puts young people at risk of communication from people who may wish to abuse, exploit or bully them.

Tackling this issue requires both accountability and an autonomous approach to security. Ensuring there is ownership over IoT security is imperative, and some institutions have appointed "digital champions" who review technology and share practices that foster innovation.

Technology, too, will play its part in managing the cybersecurity risk. Colleges and universities must implement new tools that go beyond traditional cybersecurity measures, such as User and Entity Behavior Analytics (UEBA), which identify patterns in typical user behaviour and flag any anomalies.

These kinds of solutions don't hinder employee creativity, collaboration, or speed as many clunky security systems do. Instead, they provide real-time protection and enable quick responses should a network breach occur.

Enthusiastic pupils are a huge opportunity

It's important that a focus on security doesn't take away from the bold ambition demonstrated by the education sector. In many ways, this industry in a totally

unique position. Every day, it interacts with an enthusiastic generation that gets more technologically sophisticated each year. In few other sectors is there such a huge cohort of people as adaptable and receptive to new ways of working.

This is where the opportunity lies for teachers, who can challenge the traditional way of teaching. But in order to do so, they cannot be shackled by the fear of cyber risk. Instead, education employees must continue to push themselves to investigate what other innovations can be implemented in order to enhance student learning.

There's no doubt it can feel overwhelming for many to think about how to make improvements while dealing with a demanding timetable.

However, by investing in automation technology that streamlines processes and provides protection, the opportunity of a digital workplace can become a reality. This will drive greater efficiencies, freeing up space in the day to innovate and try new things.

With the right technology in place, and a security strategy that ensures accountability for the management of said technology, there is huge potential for educational institutions to become efficient, productive and inspiring digital workplaces.

The enthusiasm for transformation is already there. With the right security strategy, I've no doubt the future of education will be bright. **crime**



Technology, too, will play its part in managing the cybersecurity risk."

CITRIX

A HIGHER PURPOSE

CNME Editor Mark Forker managed to secure an exclusive interview with **Taj El-Khayat**, Regional Director Middle East, at Citrix, to find out more about the company's new corporate rebranding - and how its leveraging its broad portfolio of technologies and solutions to elevate, empower and enable their workforce and clients to be more productive in this new digital economy.

Taj El-Khayat
Regional Director Middle East, at Citrix





El-Khayat has established himself as a prominent thought leader in the IT ecosystem over the last decade, and in a wide-ranging and in-depth discussion he perfectly articulated how Citrix was transforming the world of work.

“We’re extremely excited about reimagining and repositioning Citrix as a leader in the future of work. We’re now centering everything around the human experience and the employee experience to really enable them through technology in a way that doesn’t limit them to a particular space or location. We want to ensure that people can do their work and be innovative and creative without being restricted to anything. We wanted to remove barriers and provide people with the space to allow them to do what they do best. That has a higher purpose for us, because we completely understand that as humans become more productive, and become part of an employee workforce community, then these communities will thrive, businesses will expand and economies will grow, so that higher purpose is what is really driving us in terms of our strategy at Citrix,” said El-Khayat.

El-Khayat pointed out that a direct consequence of the COVID-19 pandemic was a huge acceleration in digital

transformation, and he believes that the resistance that may have existed prior to the global health crisis is now gone.

“We completely understand that cloud architecture is going to be key. What we’ve witnessed over the last few months is organizations really starting to take a leap of faith in a much more accelerated way than in the past in terms of its journey to embark towards the cloud. We’ve obviously got a very strong track record in transformation, and we possess the ability to move clients from on-prem legacy types of technology into the cloud,” said El-Khayat.

On October 1st, Citrix formally announced the ending of the availability of perpetual licenses. This decision also happened to coincide with the reimagination of their new corporate branding and positioning.

“What that has enabled us to do is push and accelerate our subscription-based modelling. We really want to be able to ensure that organizations are using technology efficiently – and using technology when and how they want it. We provide subscription services to our clients, which gives them greater flexibility, scalability and the ability to manage their requirements on a consumption-based basis,” said El-Khayat.

The Regional Director for the Middle East at Citrix, then explained that the third pillar



We wanted to remove barriers and provide people with the space to allow them to do what they do best.”



We're 30 years into this journey and what we really want to do is reimagine ourselves."

of their brand reimagining was focused entirely on bringing their workspace technology front and center, which is where the employee experience becomes the core of what the IT leader really wants to deliver.

"Our workspace technology, whether it's our traditional workspace technology, or our workspace intelligence leverages a lot of AI technologies and algorithms that ultimately provides us with the ability to really allow employees to work on their mission-critical tasks rather than wasting time on mundane ones. However, the question is how do we evolve that entire focus on workspace capabilities into

making workspace a platform that we can integrate with a much broader ecosystem of technologies to really make the best out of employee experience?" said El-Khayat.

There has been a lot of disruption in relation to working remotely. Many enterprises were forced to move from the compounds of their physical office environment to a virtual one in order to maintain continuity, but many were simply not equipped with the tools or technologies to make this transition a seamless one. However, this is where Citrix's workspace platform earns its stripes.

"The workspace platform is an aggregation of our technology suites that ranges from our legacy virtual desktop infrastructure, to virtual applications, end-point management, and content and collaboration. Today, organizations want to embark

upon workspace engagement for their employees to provide them seamless access and experiences across platforms, devices and clouds both on-prem and hybrid. In today's climate you don't need multiple points, you can have that digital workspace from Citrix that enables you to have that seamless integration," said El Khayat.

The charismatic El-Khayat then highlighted the close strategic partnership it has with US technology behemoth Microsoft, who have publicly announced their admiration for Citrix's digital workspace platform.

"The platform is where it becomes very exciting for us. The platform is how we leverage technology vendors to lead the way in terms of accessing and



providing the best experience for employees using that Citrix platform. Microsoft recently announced that the Citrix digital workspace is the preferred solution that they want to go to market. We've been able to leverage their own windows virtual desktop technologies, which provides them with a standard virtual desktop infrastructure, but by leveraging the power of the Citrix platform it enables them to go ahead and drive enterprise grade and highly secured access to data and applications for those users. We're trying to create endless opportunities for organizations to make it simple, efficient and extremely robust in a bid to really provide that ultimate best end-user experience to their employees," said El-Khayat.

El-Khayat claimed that the internal intent behind Citrix's reimagination is driven by what the company has witnessed since the outset of the COVID-19 pandemic, which was their technology was truly able to walk the talk when it comes to having a higher purpose and unleashing human potential.

"The way we were able to react to customers and partners needs and requirements

during the crisis was heartwarming in terms of how we enabled organizations to overcome challenges and help them maintain business continuity. However, we're 30 years into this journey and what we really want to do is reimagine ourselves. How do we want the market to perceive us, but more importantly the internal intent is what do we want to be for our employees and what do we want to be for our future employees?" asked El-Khayat.

According to El-Khayat, one of the primary objectives in terms of what they wanted to establish and create with their new brand was relevance across a diverse range of different audiences.

"One of the key things for us was that we really wanted to create a brand that is relevant across all audiences. We're an organization that has equal employment opportunities for all and we have created an environment where anybody with an intent to be innovative and creative can flourish. The X in our new brand logo represents how we're humanizing our brand. That X takes different forms because it represents the different audiences. We are a platform for everyone, and it is very important for us to create that sort of purpose where people who are part of Citrix, can drive benefit to the community at large that they serve. We want brand relevance across all audiences because we want our team to feel that higher purpose," said El-Khayat. **crme**

Nadim Abdulrahim*Global Government Industry Expert, Huawei Enterprise Business Group, Middle East*

HUAWEI

COLLABORATION AND COOPERATION

CNME Editor Mark Forker secured an exclusive interview with **Nadim Abdulrahim**, Global Government Industry Expert, Huawei Enterprise Business Group, Middle East, to learn how city administrators are coping with new trends emerging from the COVID-19 pandemic, how Huawei leveraged its Converged Command and Control Solution to help cities fightback against the virus – and how cloud is key in fueling cities of the future.

According to Abdulrahim, many global cities were simply not equipped to deal with the COVID-19 pandemic because the systems they had in place were archaic and had not been designed to be collaborative.

“One of things that we see as a big-ticket item borne out of the COVID-19 crisis is

digital transformation. There is a movement to transform governments to have their own digital platforms, specifically moving away from silo independent sub-systems per-department. This is a problem that is plaguing a lot of cities and government entities worldwide because each one has their own siloed system to

operate – and when something major happens like the current global COVID-19 situation they are simply not prepared. In this type of scenario, you need to be able to share information, cooperate and be able to adapt very quickly. If you don’t have a platform that crosslinks multiple agencies, or government departments within a city or a

nation, then it becomes very difficult to get a situation under control in an effective and efficient way,” said Abdulrahim.

Huawei are known globally as being one of the world’s most innovative companies – and Abdulrahim highlighted how they dispensed their technological expertise to help many of its customers to overcome the obstacles and difficulties they faced during COVID-19.

One of the beacons of their diverse portfolio of solutions for city administrators has been Huawei’s Converged Command and Control Solution.

Underpinning this solution is its ability to converge technologies to enhance collaboration, which historically and has been lacking within many governments in relation to its system for policing, ambulance, fire and emergency response services.

According to the Global Government Industry Expert at Huawei Middle East, there has been an absence of a unified platform with each unit having their own system.

“What we mean by collaboration is essentially linking all these entities together, so when confronted by a crisis like the ongoing COVID-19 pandemic they can rely on a system that allows them to effectively cooperate together. To enable this, you’ve got to converge all these systems together, whereas historically most government entities use a Tetra system for their mission critical communication. Tetra is a 2G-based proprietary technology, which provides



If you don’t have a platform that crosslinks multiple agencies, or government departments within a city or a nation, then it becomes very difficult to get a situation under control.”

audio communication and only allows you to send SMS’s. Whereas in our private life we either use 4G or 5G, and we can access video, audio, data capabilities and other sophisticated applications. This convergence of multimedia within the command and control industry is something we’re continuing to work on and improve – and all of it is linked on a mission-critical communications system. We provide a platform for this which is called ICP (Integrated Communication Platform) which intrinsically links everything together,” said Abdulrahim.

There is a global movement from government leaders to make their cities smarter and one of the fastest growing verticals has been the development of ‘smart cities’.

Huawei is playing a key role in making cities smarter and Abdulrahim points out how Huawei’s cloud is helping them achieve their goals.

“In relation to smart cities I think you’ve got to look at it from a macro perspective and examine the bigger picture. Firstly, you’ve got a lot of devices providing information such as cameras, traffic enforcement & IoT sensors, drones and so on, which you want to send over an infrastructure or a pipe. This infrastructure will be feeding data to a cloud, whether it be a city or a government cloud, where you run the applications to enable processing and decision making. We look at it from the perspective of device, pipe, cloud and application. You want to capture the data from all these devices, transport it over

an infrastructure to the cloud where you can then process it using specific applications,” said Abdulrahim.

He added that once you have it in the cloud you have an open platform in which you can essentially link anything, and stressed that when you’re looking at the bigger picture you also need to consider the impact of technologies such as 5G and AI will have on the development of a smart city.

“To take it one step further and improve government productivity, enhance their quality of services, and provide a paperless services environment then the cloud has to be intelligent – and it has to have the ability to provide automated services – and for that particular part of the arena we provide Enterprise Intelligence. Enterprise Intelligence is AI – but is adapted and customised by the customer for their specific requirements and we provide this on the Huawei Cloud as a service,” said Abdulrahim.

The charismatic and dynamic executive concluded our brilliant conversation by reiterating the importance of data and how it is fueling the digital economy that we now live in.

“The more data you have at your disposal ultimately allows you to make better-informed decisions. We call it ABC. The A stands for Artificial Intelligence, the B stands for Big Data and the C is for cloud, because these three together are basically the digital transformation of the future combined with 5G as a transportation medium,” said Abdulrahim. **enme**

MICROSOFT

MANAGING RISK

CNME Editor Mark Forker managed to secure an exclusive interview with **Bharat Raigangar**, GM – Business Head, India, Middle East & Africa at Wipro, and **Sanchu Sankar**, Chief Architect, Identity and Security, Microsoft Consulting Services, EMEA, to find out how both entities are leveraging their expertise to enhance its cloud threat management capabilities through a cloud-native SOC for single or multi-cloud customers.



BHARAT RAIGANGAR
GM – BUSINESS HEAD,
INDIA, MIDDLE EAST &
AFRICA AT WIPRO



SANCHU SANKAR
Chief Architect, Identity
and Security, Microsoft
Consulting Services, EMEA

Many security experts have claimed that a SOC (Security

Operations Centre) can help to enhance and protect government entities and large enterprises from cyber threats and attacks? However, in your expert opinion, what are the unique capabilities of a SOC that makes it so essential for network security?

Bharat Raigangar: Managing security risk from actual and anticipated risks to a specific organisation is often a dynamic endeavour. Security risk can be affected by frequent changes in threats and adversaries (or awareness/knowledge of them) such as the attack techniques they use, the controls available, and the effectiveness of those controls.

In a defensive capacity, you need to have the capability for the prevention of incidents through proactive threat analysis, monitoring for threats and adversaries, real-time detection and historical trending, response co-ordination and decision support, providing situational and context awareness and operations and maintenance of defensive technologies that provides integrated intelligence vertically and horizontally.

A standard and consistent incident response plan should be created and tested. This should define all roles of personnel as well as phases of incident handling/management from detection to post-incident review.

To be successful in managing risk, you need to have effective people processes and tools to operationalise intelligence, automate investigation and response workflows and a “cloud-native mindset to security”.

SOC capabilities have never been the same since the origin of SOC in organisations and today the essential capabilities include monitoring, detection, response, threat intelligence, analytics, automation, vulnerability and compliance management among others.

One of the key strengths of a SOC would appear to be its ability to incorporate cooperation between man and machine, but how do you create a Modern SOC – and what are the defining characteristics of a Modern SOC?

Bharat Raigangar: As organisations operating boundaries significantly changed with digitisation, cloud, and mobility, so did the threat landscape. SOC modernisation initiatives are on the rise across the industries to augment advanced capabilities in a much more unified way to combat the sophisticated nature of adversaries.

The reality is that a good cyber hygiene is hard to manage because of the sheer volume of controls and the challenge of determining which controls are going to work well, or possibly not, within your environment.

You need capabilities that provide intelligence across specialised tools – providing high quality alerts, end-to-end investigation capabilities and

“

A standard and consistent incident response plan should be created and tested.”

remediation. You also need to have a unified View across all the different tools and controls – unified alert queue, Log detection using UEBA/ML. Integrated intelligence is key.

SecOps usually evolves by adopting specialised tooling and cloud-native analytics. Most investigations start with EDR capability (regardless of alert source), and then often pivot into identity and email/software as a service (SaaS) capabilities’.

You also need upgrading to a Cloud-Native SIEM, such as Azure Sentinel, that can go further and correlate insights from different security tools such as Microsoft Defender for Endpoint, Microsoft Cloud App Security, Microsoft Defender for Identity, Microsoft Defender for Office 365, etc.

Modern SOCs need to demonstrate the effective functioning of these advanced threat detection capabilities in an integrated way and leveraging inbuilt machine learning techniques, ability to contain and isolate at speed, cloud sandboxing to detonate and understand the malware behavior, User Entity & Behavior Analytics (UEBA), external threat intelligence, hypothesis basis advanced and proactive threat hunting and most importantly advanced security orchestration and automated response capabilities (SOAR).

Wipro has also been investing heavily in growing its modern SOC as Cyber Defense Center (CDC) footprint geographically and their intrinsic technology processes and talent readiness to meet

the current and future threats that customers would face.

The current model of the CDC supports 24/7 monitoring, contextual threat intelligence, threat detection through advanced correlation, incident management workflow, compliance reporting, and other features discussed above.

The CDC is underpinned by the following operating principles:

- Manage the growth without compromising on agility
- Execute the defined SOPs to the highest standards
- Maximise the value of the tooling investments for detection and response
- Win together – disseminate collective wisdom to upstream (partners, CERTs) and downstream (customer) stakeholders

Microsoft and Wipro have been trusted partners for over 20 years. Can you outline to our readers how important this collaboration has been for both entities and what value you both derive from each other?

Sanchu Sankar: Relationships like this are critical in delivering the best to our customers and to solve challenging problems in security. With Wipro's 20+ years of vast experience and deep expertise in cybersecurity and with Microsoft's strong commitment to cloud-based security technologies continuously innovate and enhance security at every layer, has helped take the alliance to assist customers right from the value conversations, strategy, solutions and technology adoption.

As discussed earlier, to be successful in managing risk, you need to have effective people, processes and tools to operationalise intelligence, automate investigation and response workflows and a “cloud-native mindset to security”.

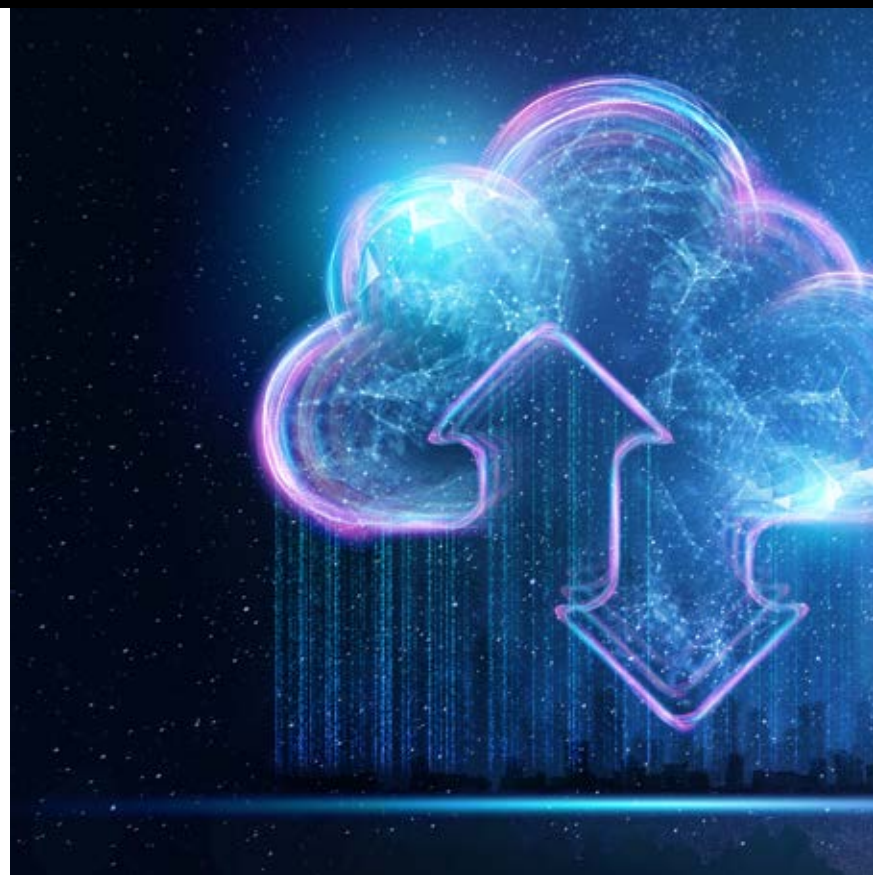
This is where we are working together as trusted partners for our customers in helping to modernise your Security Operations Center by leveraging the power of cloud-native security tools such as Azure Sentinel, Microsoft Defender – and bringing in a unified security posture across the entire organisation.

In addition to the tools, through this strategic partnership, Microsoft is bringing in experts from consulting services supported by Wipro Advisory to provide technical leadership and to provide advisory services across the complete lifecycle.

Recognising the importance of having an effective people and process model to manage your modern SOC, Microsoft is also bringing in experts to assess and provide recommendations on your current major incident management, problem management, event management processes, governance model, SOC continuity strategy, change management, SOC communications and to support upskilling Security IT managers on how to lead their employees through this modernisation drive.

In addition, Wipro is also a Microsoft Intelligent Security Association (MISA) member to help develop customer solutions in consolidating and transforming security solutions and services to accelerate the adoption through highly integrated and matured managed security services.

The Microsoft Intelligent Security Association (MISA) is





an ecosystem of independent software vendors that have integrated their solutions to better defend against a world of increasing threats.

Wipro is also the leading Global Managed Security Service Providers (MSSPs) and provides feedback on the security technologies which helps in feature enhancements and holds access to new innovations under the NDA while piloting preview features.

In December 2019, Wipro announced the launch of its advanced SOC services which are powered by Microsoft Azure Sentinel? What sort of impact has this solution had in the IT security ecosystem over the last 12 months?

Sanchu Sankar: The launch of Wipro advanced SOC services powered by Microsoft Azure Sentinel, the next-generation security operations with cloud

and AI, has been a game-changer.

It has led to several proof of concepts, SOC modernisation conversations, pilot programs and we are now seeing some of the engagements go -live.

With Microsoft, Wipro is enhancing its cloud threat management capabilities in the form of an adaptive, intelligent cloud native SOC for single or multi-cloud customers.



SOC modernisation initiatives are on the rise across the industries to augment advanced capabilities in a much more unified way to combat the sophisticated nature of adversaries.”

As part of this integration, Wipro is offering managed cloud SOC services with built-in artificial intelligence (AI) and orchestration capabilities for rapid threat detection and response for its clients across hybrid cloud environments.

In addition, AI-based capabilities of Wipro HOLMES® are being used to measure the risk factors against compliance standards.

What differentiates this SOC solution developed jointly by Wipro and Microsoft from other similar solutions being floated in the market?

Bharat Raigangar: The joint MDR (Managed Detection &

Response) offering developed by Wipro and Microsoft consulting services, is primarily aimed at large organisations as they scale and remove complexities to transform from their current state to future state.

This will involve co-existence, migration, integrations, customisation by leveraging product engineering teams, augmenting new capabilities as per modern SOC needs, managed SOC services consolidation and transition.

As discussed earlier and to reinforce the message, to be successful in managing risk, you need to have effective, people, process and tools to operationalise intelligence, automate investigation and response workflows and a “cloud-native mindset to security”.

This is where our strategic partnership brings in value and end-to-end SOC operations to customers by leveraging the power of Cloud-native security tools from Microsoft, experts from Wipro Consulting Services to develop a modern SOC strategy, roadmap, and enablement of technologies.

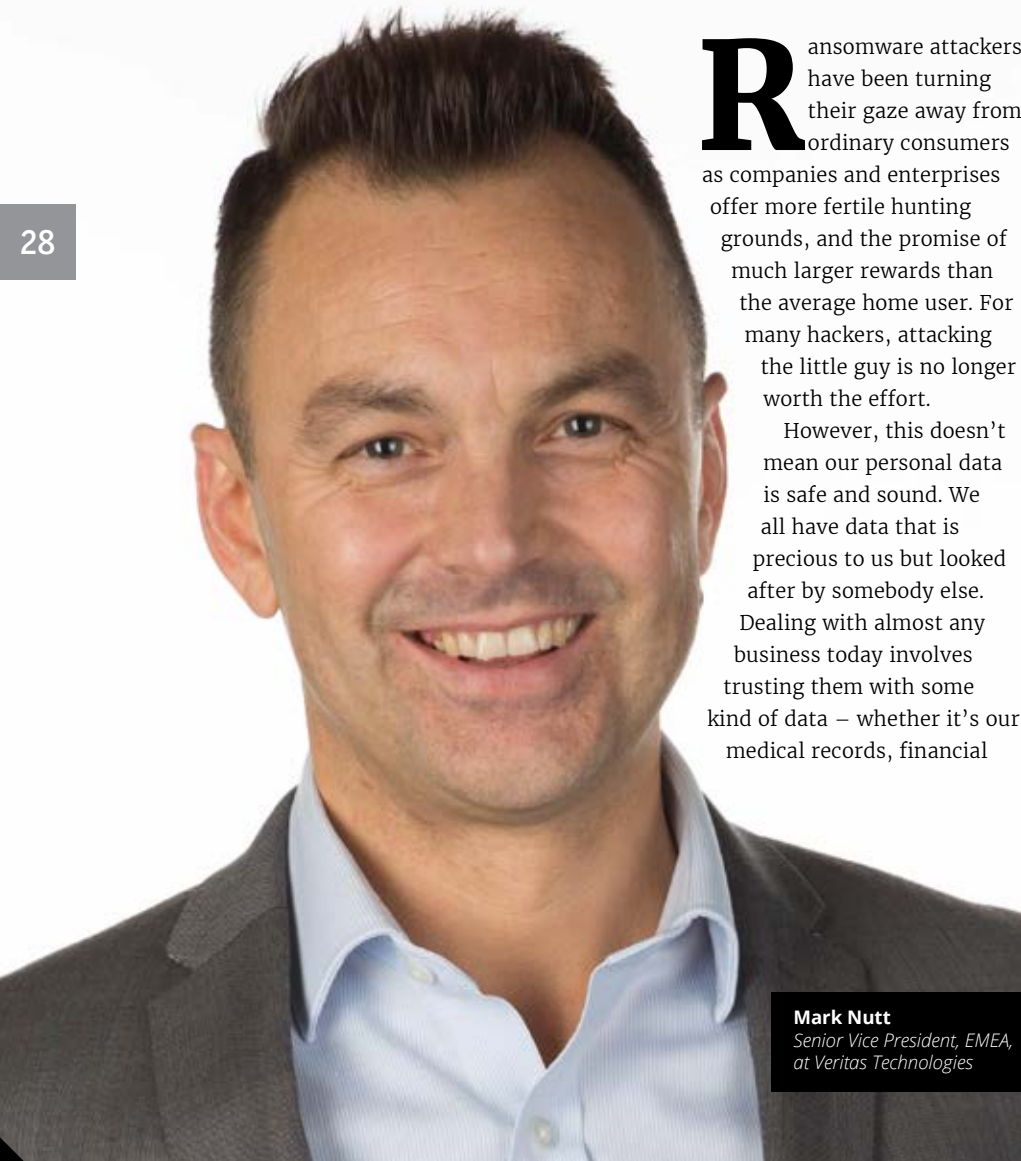
In addition to this, addressing people and process aspects to drive an efficient and modern SOC operations and Wipro bringing the expertise of SIEM and NDR technologies, unified SOC for IT, OT & IoT along with the library of use-cases and automation playbooks and ability to deliver managed SOC services from Wipro's established global Cyber Defense Centers across US, UK, Europe, Australia, India, and the Middle East. **crme**

VERITAS

RANSOMWARE: WHAT IS YOUR DATA WORTH?

Mark Nutt, Senior Vice President, EMEA, at Veritas Technologies, has written an exclusive op-ed for CNME, in which he examines the evolving behaviours of ransomware attackers and how they've shifted their focus from ordinary day consumers to large multinationals.

28



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

Mark Nutt
Senior Vice President, EMEA,
at Veritas Technologies

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% 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%) of consumers think that businesses should negotiate with cybercriminals. Similarly, just 27% 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.



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.”

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.

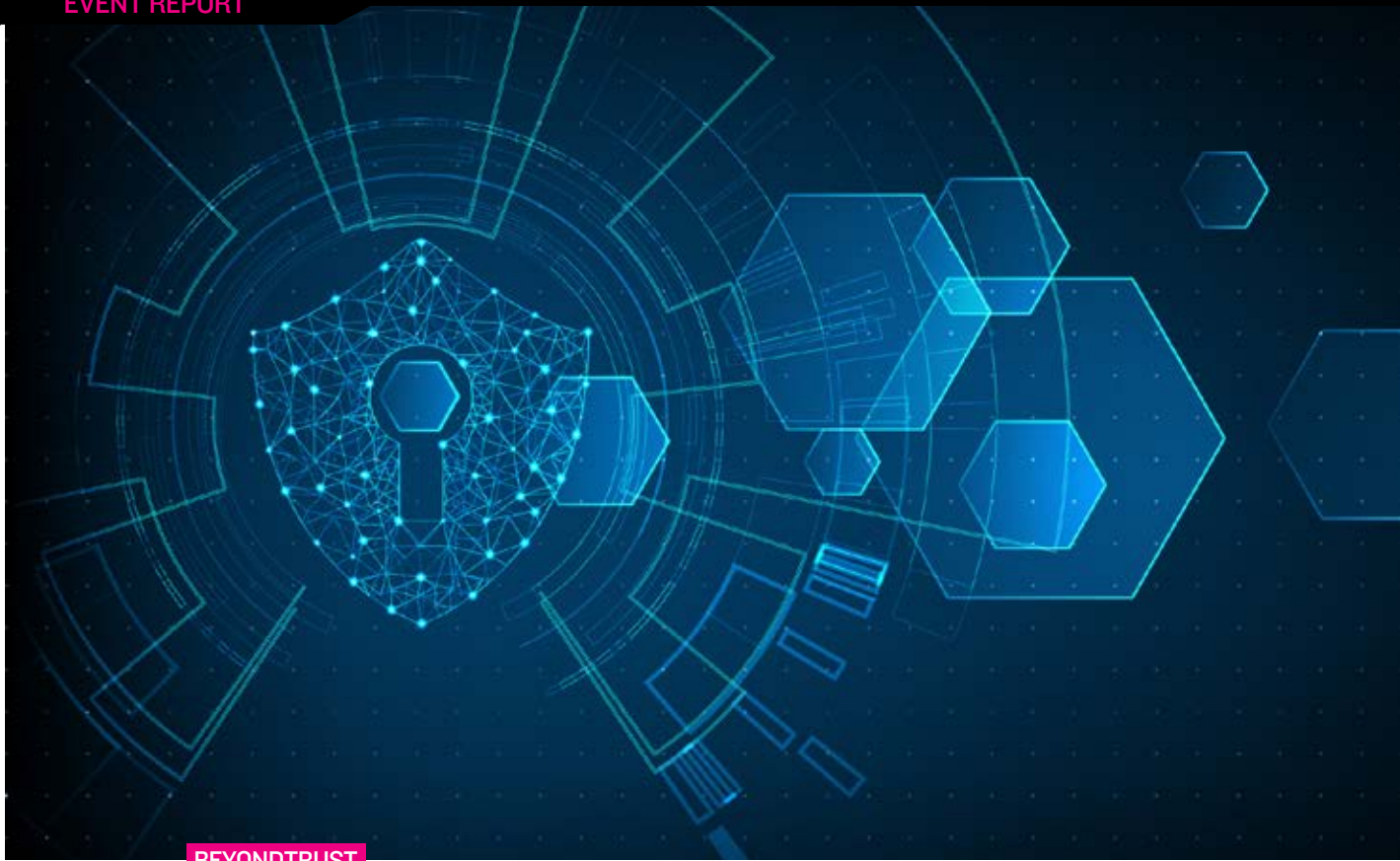
Ransomware attacks on ordinary consumers are rarer now, but they still happen. To avoid being caught out, be diligent when it comes to what emails you open and which links you click, and ensure you're using up-to-date antivirus software. But you should always work on the assumption that a new virus or 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. **crime**



BEYONDTRUST

30

LEAST PRIVILEGE FOR MORE SECURITY

Cybersecurity leader BeyondTrust hosted a virtual discussion this month to unravel the increasingly complex world of digital security - and explain the benefits of Least Privilege security models. The online event was hosted in partnership with CPI Media Group and was attended by technology decision-makers from around the region.

The virtual presentation and discussion drew technology experts from enterprises around the region to discuss the rapidly changing threat landscape and highlight the importance of a Least Privilege model in the protection of data and mission-critical applications.

John Hathaway, Regional Vice President, BeyondTrust, opened

the event with an eye-opening overview of the role of Least Privilege in the current attack chain scheme.

“The way that organisations would ideally treat cyberattacks would be to prevent them completely. These days, it is almost impossible to accomplish that,” explained Hathaway. “The number of breaches today is beyond any expectation, and the speed at which breaches are

happening is not slowing down. So, it has become about how we manage risk, what strategies do we have in place, and what tactics do we have to limit a bad actor’s ability to inflict damage.”

One of the ways to mitigate the damage caused by cybercriminals, said Hathaway, is to adopt a model of Least Privilege. Least Privilege models limit access to data and applications, providing only those



John Hathaway
Regional VP, BeyondTrust

privileges which are essential to perform intended functions.

“The principle of least privilege is a common term in security, while most organisations recognize the concept, they fail to fully grasp it and realize its powerful risk-reduction capabilities,” said Hathaway. “To build and maintain an effective security posture, it is imperative to transform this theory into a strategic and tactical tool for properly protecting critical assets within your organisation.”

Adopting a Least Privilege model can significantly reduce the attack surface on endpoints. Removing admin rights mitigates the risk of over 80 percent of Microsoft’s Critical Vulnerabilities, noted Hathaway. Least Privilege also allows unknown privileged applications to be quickly managed while keeping even the most demanding end-users productive.

In addition to a more secure cybersecurity profile, Hathaway outlined strategic, managerial,

and operational benefits from adopting a model of Least Privilege. Least Privilege environments see improved day-to-day experiences for employees, better resource allocation and operation direction, and greater agility in future-planning and contingencies, according to Hathaway.

Michael Byrnes, Lead Solutions Engineer, Middle East, and India for BeyondTrust then took the screen to outline the practical steps to Least Privilege implementation. Byrnes reviewed in detail the best practices for IT professionals seeking to bring a policy of Least Privilege to their organizations.

“Underlocked environments means that while the users may be productive, the overall security is weakened and the threat is always escalating. Overlocked environments where all users are locked down to standard user accounts can be unproductive, and provides for a poor user experience that can lead to privilege creep and increased support costs,” Byrnes explained the pros and cons of security policies.

Unpacking BeyondTrust’s integrated portfolio, Byrnes noted the company’s offerings of privileged password management, endpoint privilege

management, and secure remote access management. These offerings, the executive explained, can be implemented on-premise, in the cloud, or in hybrid environments.

“We offer Universal Privilege Management for a holistic deployment,” said Byrnes, noting that Endpoint Privilege Management, the topic of the day’s discussion, is a key pillar in BeyondTrust’s integrated offerings. “We implement true Least Privilege, and can with rapid deployment, we can sometimes implement the solution overnight, or in just a few days.”

Byrnes outlined practical steps all IT leaders need to take before deciding to deploy any Privilege Management solution. Key questions on funding, key drivers, benchmarks, and timelines should be addressed internally, with the help of experts like BeyondTrust. Key stakeholders should be identified, and legacy technologies should be assessed to optimise integration.

Universal Privilege Management enables users to work productively without admin rights, explained Byrnes. Once the solution is deployed, organizations can immediately prevent attacks, achieve compliance, gain increased visibility into user activity, and operate efficiently at scale.

Organisations looking to implement a policy of Least Privilege stand to gain significant ground in the fight against cybercriminals. BeyondTrust is able to implement Least Privilege solutions quickly and efficiently while improving the end-user experience. **cnme**

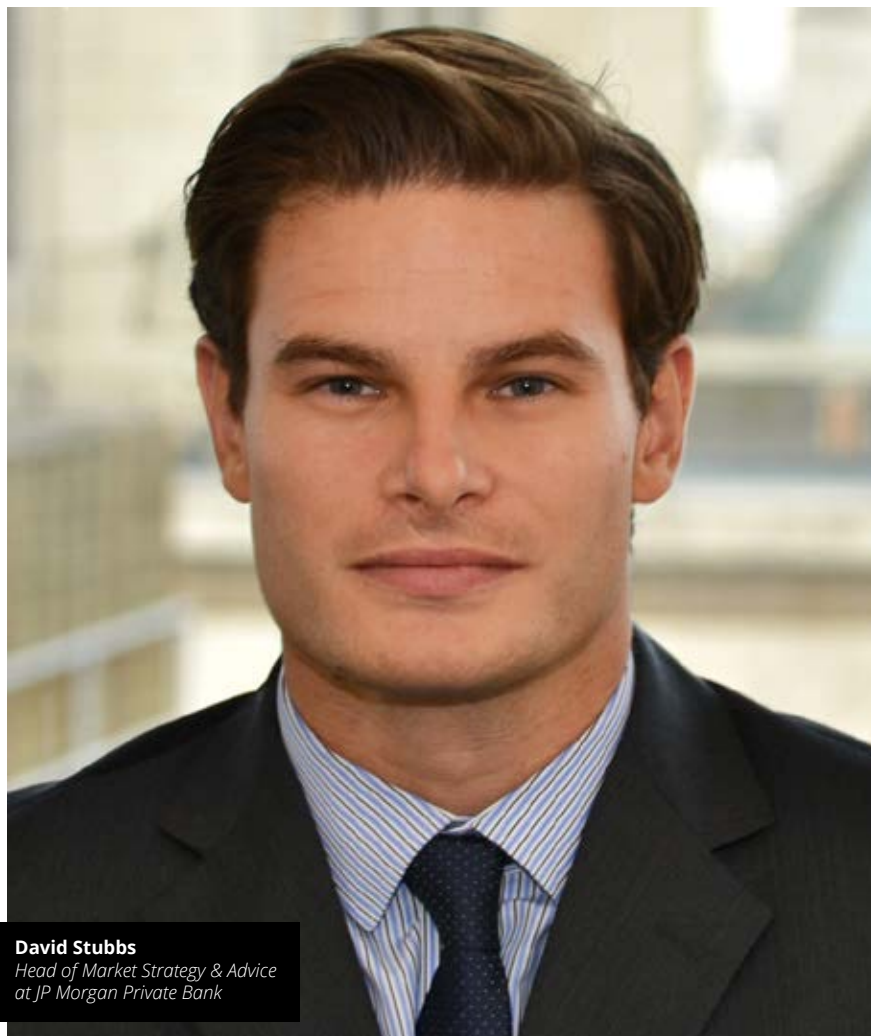


We offer Universal Privilege Management for a holistic deployment.”

JP MORGAN PRIVATE BANK

TRANSFORMING FINTECH

David Stubbs, Head of Market Strategy & Advice at JP Morgan Private Bank has penned a detailed op-ed which takes an intrinsic look at the impact digital transformation has had on the already burgeoning FinTech sector.



David Stubbs
*Head of Market Strategy & Advice
at JP Morgan Private Bank*

In a thought-provoking feature, Stubbs highlights the rapid increase in e-commerce as consumers spending habits continue to evolve in an era being termed the 'on-demand' digital economy, where the potential opportunities are, and projects we will see more disruption in the industry in 2021.

For years, cash transactions were favored by consumers worldwide, as 75% of them conduct most of their transactions in cash.

Physical payments were deemed secure and reliable, and e-payments were deemed as a back-up and last resort. Even though this notion began to shift a few years back, it was the year 2020 that caused a major change of hearts.

This year, 71% of consumers in the UAE reported an increase in using digital payments, even when shopping in-store. For good reason, digital transformation has reached the financial industry and a FinTech revolution is surely on its way.

According to MaGNI^{TT}, the UAE emerged as the largest FinTech hub in the Middle East and Northern Africa (MENA) region with a total of \$237M invested in 181 deals between the period of 2015–2019.

Today, and as the world defines a new normal, the FinTech industry is preparing to benefit from the virtual lifestyle we have had to adopt. Regionally, the UAE is poised to reach a record-high of USD2.5/- billion by 2022, taking pole position in the Fintech market according Clifford Chance Report.

What is FinTech, exactly?

Financial technology is the umbrella term for products and services that use the internet, software, mobile devices, or cloud capabilities to enable individuals, businesses, governments, and others with anything money related. The technology is being used in crowdfunding platforms, cryptocurrency, mobile payments, insurance, and stocks.

Where are the potential opportunities?

As financial services are transformed, new business models are generating significant growth. Consider, for example, the state of electronic and contactless payments, digital banking, and artificial intelligence (AI)-based insurance solutions.



Having a tech-savvy population, the UAE thrives on digital advancements and novel technologies. So it is no surprise that cashless payments are on the rise across the country, and Fintech investments are catching headlines.

According to Dubai International Financial Centre, 50% of the Middle East, Africa and South Asian (MEASA) population have limited or no access to financial services. This provides a promising opportunity to provide these fast-growing markets with

an easier and more accessible banking option – such as digital banking and financial technologies.

Offering digital banking solutions to markets where physical bank branches are scarce or hard to reach, or banking without a minimum account balance is an opportunity worth exploring.

More FinTech growth and disruption on the way

Digital transformation is a megatrend across the globe that already has disrupted financial services—but even more disruption can be expected. Worldwide, we have been moving away from the status-quo of finance and towards exciting transformation. It would be worth exploring investments in the FinTech industry as growth is certainly on the way. **crime**



Digital transformation has reached the financial industry and a FinTech revolution is surely on its way.”

AIO NETWORKS

TRUST NOBODY

A10 Networks, a global leader in cybersecurity, this month hosted a virtual roundtable with the aim of discussing the benefits of implementing a Zero Trust policy in the current threat landscape. The online event was hosted in partnership with CPI Media Group and was attended by IT decision-makers from around the UAE.



encryption designed to protect networks, leaves IT professionals with a choice: either encrypt traffic and risk threats from bad actors that can take advantage of the TLS blind spot, or leave traffic unencrypted, which is both a security risk and oftentimes a compliance violation.

In his overview of the cybersecurity threat landscape today, Baghir noted some startling statistics. “We are seeing a 650 percent increase in trojan-based malware threats,” he said, “and the average cost of a data breach today is USD \$3.92 million.” A number of these attacks, warned Baghir, are enabled by internal threat actors.

The impact of these threats can be devastating, Baghir went on, and can result in lost revenue, investigation costs, and brand damage. Non-compliance with regulations like GDPR, for example, could result in fines and sanctions that could severely affect an organisations mission and bottom line.

Ransomware is particularly insidious, as internal threat actors are not always aware of the damage they cause, explained the executive. “This could be a normal employee or anyone

A10 Network’s online event and discussion was attended by technology leaders from key industries in the region. Executives from A10 Networks highlighted the need to adopt Zero Trust policies, as well as its importance in maintaining compliance as regulations continue to develop in the MENA region and around the world.

Adil Baghir, Senior Pre-sales Consultant, A10 networks took the screen as the day’s featured speaker and was joined shortly after by A10 executives Ehab Halablab, Regional Sales Leader,

and Hasan Darwish, Regional Sales Manager for an interactive panel discussion.

“We are seeing many of our customers investing heavily in their IT security infrastructure. However, attackers are still taking advantage of a blind spot to take advantage of organisations and compromise their networks,” said Baghir, referring to bad actors who actually leverage TLS encryption against enterprises to conceal malware delivery, eavesdrop on communications, and exfiltrate data undetected.

The fact that cybercriminals are actually leveraging the



Adil Baghir
Senior Pre-sales Consultant, A10 Networks

who has access to your network, including remote workers,” he said, noting the growing pool of remote workers since the start of the COVID-19 pandemic.

To solve these security issues, A10 Networks advises organisations to take on a Zero Trust model. A Zero Trust model is built on the axiom “trust nobody.” In a Zero Trust model, networks are redesigned into secure micro-perimeters and user privileges are limited. This allows for increased visibility into users, data, and workflows, as well as improved detection and response times through analytics and automation.

Existing security solutions, said Baghir, are inefficient, expensive, and complex. “These systems can be costly, and not purpose-built, need an inflexible deployment that can be disruptive, and often have difficult operationalization.” Clearly, a fresh look at cybersecurity is needed to address

today’s evolving cyber threats.

To this end, A10 Networks offers its SSL Insight solution. With SSL Insight, A10 leverages hardware ASICs, which are much faster at decryption and reencryption, to offload the security responsibility from enterprise devices. This allows devices across organisations to benefit from centralised decryption with hardware ASIC acceleration.

With so many security vendors on the market, A10 Networks differentiates itself



In a Zero Trust model, networks are redesigned into secure micro-perimeters and user privileges are limited.”

in myriad ways. They offer a flexible deployment model that can accommodate most network designs, they remain vendor agnostic, provide full proxy architecture, and for high-security environments like government organisations, they provide Hardware Security Module support. Additionally, A10 Networks supports Dynamic Port Inspection and ICPA protocols.

A solution of any kind is only as powerful as its ability to be deployed and integrated into existing infrastructure. “The solution can also be integrated seamlessly into any network as a Layer 2 or 3 device,” Baghir assured the attendees. “It can also be deployed as a transparent proxy. It can be easily integrated with any kind of proxy deployment.”

Following Baghir’s presentation, A10 executives Ehab Halablab, Regional Sales Leader, and Hasan Darwish, Regional Sales Manager for joined the discussion to navigate practical implementation questions from the event’s attendees.

Halablab concluded the discussion by underlining the importance of end-user awareness. “Zero Trust attempts to fix the problems and patch the holes associated with current cybersecurity strategies. At the core of it, Zero Trust is, of course, trust nobody. Employees may not even know that they are causing damage, so there needs to be a dedicated program to increase employee awareness,” he said. This is particularly true, the executive noted, this year as organisations implement remote and hybrid-remote working models. **cime**

HUAWEI

HUAWEI CLOUD IS CREATING GLOBAL OPPORTUNITIES

In an exclusive op-ed, **Omar Akar**, Regional Vice President and Managing Director, Cloud and AI Business Group, Huawei Middle East, highlights how Huawei Cloud is paving the way for a vast array of global opportunities in the IT ecosystem.

Cloud computing is booming. The changes in the technology landscape have allowed it to flourish and become a key part of corporate IT strategy alongside some of its more advanced technologies such as AI and IoT.

The ability to connect to a wide range of data sources across the internet in a fraction of a second was unthinkable a few years ago. The technology is now so well embedded that cloud-based operations are a cornerstone for tens of thousands of companies across the world, spearheading their growth and expansion process.



Omar Akar
Regional Vice President and Managing Director,
Cloud and AI Business Group, Huawei Middle East



The ability to connect to a wide range of data sources across the internet in a fraction of a second was unthinkable a few years ago.”

Huawei is playing a key role in the growth of cloud computing, building an ecosystem to include partners of different types to examine innovative ways to deploy cloud technology.

The growth of cloud is driven by the rapid increase in Internet usage worldwide according to Mark Chen, Director

of the International Business Department at Huawei Cloud. The number of Internet user exceeds 380 million in the Middle East and North Africa, 480 million in Southeast Asia, and 450 million in Latin America.

Despite these numbers, there are still vast opportunities to be explored. Huawei Cloud is leveraging its technical edge, its knowledge, and partner programs to provide support for internet companies that want to take advantage of the opportunity.

Gaming firm NetEase has also been able to expand rapidly thanks to the robust cloud services Huawei provides. NetEase-produced online game “Conqueror’s Blade”, which runs entirely on Huawei Cloud nodes outside of China. Such cloud service nodes are also deployed in Latin America to provide network coverage there.

Huawei’s services are used across the world. Huawei has deployed more than 2,500 content delivery and POP nodes across the globe along with 45 availability nodes delivering 210+ advanced services to accelerate digital transformation of all industries.

Huawei is also proud to announce that these services will be launched in the Middle East this November.

While these are just some of the many successful stories, Huawei looks to provide partners with even more assistance both financially and technically under its HMS Ecosystem Support Program. Incentives include development and testing coupons plus cloud resources and migration tools. **enme**

CNS

MANAGED SERVICES

Hatem Hariri has established himself as one of the most prominent thought-leaders in the IT ecosystem, and in this op-ed the Managing Director at CNS, outlines some of the differentiating factors that separate the IT leader from its market rivals.



Hatem Hariri
Managing Director at CNS



CNS can be responsible for all or parts of a client's technology systems, as per their Service Level Agreement (SLA)."

Today's business leaders tend to overlook the competitive advantage of a digitalised enterprise, but astute enough to delegate their managed technology operations to an expert organisation that specialises in handling these responsibilities.

As a leading information technology and banking solutions partner in the Middle East, and with 30 years of experience in delivering innovative solutions and professional outsourcing services, CNS also provides Managed Technology services.

While there's no denying that technological innovations

nearly always improve the way a business can be run, there are few companies with the resources needed to keep abreast of increasingly demanding, ever-evolving market.

Even those that do are justly apprehensive about outlaying precious capital on technologies today that might well be redundant tomorrow.

As the company uses owned resources there's little need to invest in additional hardware. And since applications are used on an as-needed basis, every managed solution can be scaled up or down as needed on a pro-rata cost to company

This scalability not only increases efficiency in pricing, but competitiveness as savings in operational costs can be passed over to their clients' customers.

We at CNS can be responsible for all or parts of a client's technology systems, as per their Service Level Agreement (SLA).

CNS Managed Service solutions offer a wide range of benefits to organisations of all sizes from round-the-clock monitoring to fast-tracking resolutions and reporting processes, enabling better data collection and security, while introducing big saving on cost with significant SLA agreement

"It's an honor that so many of our most valuable clients have put the responsibility of their information systems in our expert hands. I see CNS managed services becoming an essential cornerstone to our value proposition as a cost-effective way to help lead our clients along their journey to full business digitalisation. **crme**

Huawei CloudEngine Series Data Center Switches

Named **a Leader** by Forrester

Leading Data Center Networks into the Intelligence Era



CloudEngine Series Data Center Switches



DCN Solution



Twitter



LinkedIn



Facebook

Source: The Forrester Wave™: Open, Programmable Switches For A Businesswide SDN, Q3 2020



GovTech

NOVEMBER 2020
TAHAWULTECH.COM

INDUSTRY



THE FUTURE OF WORK

THE FUTURE OF WORK

In this month's edition of GovTech, we examine how the combination of disruptive technologies and the COVID-19 pandemic has fundamentally reshaped the way we work, when we work and where we work – and we attempt to explore what the future of work will look like in Industry 4.0?

40

IT leader Citrix compiled a comprehensive research report which examined what the future of the workplace will look like – and explores how people and technology will pioneer new ways of working in what is becoming an increasingly connected and data-driven digital economy.

As a direct consequence of the ongoing global health crisis enterprises have been forced to revolutionise the way they work and this new hybrid model of work that has been developed is here to stay. The employee experience has changed overnight and now the role of business leaders and employees

is to reimagine what the future will be.

Drawing on the perspectives of academics, business leaders and employees across the U.S. and Europe, Citrix commissioned an ambitious two-part research study called **Work 2035** that sought to imagine work in the year 2035.

Where might the opportunities lie? What might stifle progress? And how might people use technology to generate the best outcomes—both for their organisations and themselves?

In the first stage of their forensically detailed **Work 2035** report they were able to determine and establish two critical axes needed to provide a

solid foundation for the future of work, and they were workers replaced vs. workers augmented with technology, and a centralised world of work vs. a distributed world of work.

Citrix leveraged these axes to create four distinct scenarios for the world of work in 2035.

The respondents of the Citrix **Work 2035** survey were emphatic in the fact that they firmly believe that the integration and implementation of new technologies will increase productivity and give employees a higher purpose.

The report said, “Seventy-seven percent of all surveyed professionals believe that by 2035, AI will significantly



73%
of business
leaders
believe that
tech and AI
will make
workers
at least
twice as
productive
by 2035.”

speed up their decision-making process – and respondents also agreed that in the future, tech interfaces will increase human productivity and performance. But our research also revealed a profound gap—a digital disconnect—between how business leaders and employees perceive the future of work. 73% of business leaders believe that tech and AI will make workers at least twice as productive by 2035. 39% of employees believe that tech and AI will make workers at least twice as productive by 2035.”

One of the most interesting insights to emerge from the Citrix **Work 2035** Report was that there is two very different perspectives in terms of what the future of work looks like through the lens of employees and business leaders.

The report said, “Even though over 3/4 of business leaders believe that organisations will create functions like AI management departments and cybercrime response units, fewer than half of employees anticipate these business units by 2035. Whereas most business leaders anticipate a world of strong corporate structures powered by a flourishing human-tech partnership, employees foresee a much more fragmented world, with big corporations no longer dominant, and many roles replaced by technology.”

ServiceNow is a digital workflow company that makes work, work better for people. It has enjoyed phenomenal

success since its inception and its primary objective as a company is to continue to reshape, reimagine and rethink the employee and workflow experience on a global scale.

It has launched its new Workplace Service Delivery solutions, which delivers seamless digital experiences to employees wherever they are, driving employee productivity and satisfaction in a rapidly changing workplace landscape.

Workplace Service Delivery provides organisations with a single solution that enables employees to use their connected devices to reserve workspaces, including desks, conference rooms and collaboration spaces.

The solutions enable employees to easily request room configurations, catering, AV support and more, while providing corporate real estate teams with the analytics and utilisation data they need to optimise spend and service levels.

With employees and businesses opting for distributed working models, ServiceNow provides organisations with a seamless service delivery model for employees when they want to return to the office. With Workplace Service Delivery, ServiceNow expands its unified employee service experience across HR, IT, legal and now workspace services.

“After having adapted to a new world of remote work over the last six months, businesses must now shift from crisis to planning mode,”

said Blake McConnell, senior vice president of employee workflow products, ServiceNow. “This includes reimagining the processes and systems that keep employees safe and productive in a distributed environment. Powered by the Now Platform, Workplace Service Delivery is designed to be the foundation for modern, connected employee experiences in all work environments, helping enterprises optimise how they manage workplaces and workforces going forward.”

“Over the next year, two-thirds of companies will invest in automation related to their facilities. In addition, one in five companies worldwide will add new applications to address needs uncovered by the COVID-19 pandemic, including space utilisation, desk reservations and visitor management,” says Juliana Beauvais, research manager in IDC’s enterprise applications practice focused on enterprise asset, facility, and real estate management. “Moving forward, it’s more critical than ever for organisations to focus on the employee workplace experience.”

Companies like Citrix and ServiceNow are going to play key roles in reimagining the future of work and will cultivate its technologies to make these predictions a reality, whilst it can be hard to predict the future, one thing is for sure and that is the world of work has changed and the opportunities going forward are boundless. **cme**

ERICSSON

UNLOCKING THE POTENTIAL OF ESIM

Said Zantout, Head of Solution Area OSS, Core and Cloud at Ericsson Middle East and Africa has penned an in-depth op-ed on the potential and capabilities eSIM can have for consumers in our digitally driven economy.

42



Said Zantout
Head of Solution Area OSS, Core and Cloud
at Ericsson Middle East and Africa

eSIM has become a hot topic among device manufacturers and its increasing role in the industry is clear – as device manufacturers benefit from lower costs and more space on the processing board. Moreover, eSIM helps service providers to generate new revenue streams, and a future of billions of IoT connected devices

During 2019, two major smartphone manufacturers announced several of their models were now equipped

with eSIM functionality. In 2020, many more are following suit. By 2025, GSMA estimates that more than 2 billion eSIM devices will be shipped. This is a strong incentive for the industry to go for eSIM.

But what about consumers like me and you? What can eSIM bring to us?

To answer these questions, Ericsson ConsumerLab has run a market research study, revealing key insights which means customers are ready to take the next step and pay for eSIM services:

- Cellular connectivity for additional devices is the top application of eSIM that consumers are interested in. 6 in 10 want to connect their laptops to cellular connectivity, yet very few do it today.
- Every SIM card is problematic, main issue being related to the ever-decreasing size of SIM cards. For consumers, eSIM represents peace of mind, for example 45% mention having access to multiple operators in the same smartphone for emergencies.

- 6 in 10 smartphones users are interested in eSIM. However, 40% of them have locked smartphones, while 73% have post-paid plans with a contract.
- 29% of smartphone users would consider buying a smartwatch with cellular connectivity if the process of enrollment with the operator was seamless.

According to the report, there are four main eSIM benefits for consumers. Firstly, it excels in connectivity.

Consumers say that the need to switch between operators depends on the connectivity performance at various times and places. If the connectivity is great, one operator is enough, so when is switching between operators relevant to consumers?

The results took us by surprise – 75% would activate a reasonably priced plan on top of their existing one to ensure access to connectivity.

eSIM is not about swapping back and forth between operators for the sake of just saving a couple of dollars a month. eSIM is about peace of mind! Even smartphone users whose expectations regarding network quality are met want to be able to shuffle between operators. Peace of mind is more important than loyalty when it comes to places out of reach and emergency situations.

The second benefit is travel specials, which refers to connectivity in the context of travelling abroad. In fact, 1 in



Travelers that use local SIM cards abroad are particularly interested in a service that would ease the process of choosing the optimal connectivity offering.”

2 yearly travelers connect to mobile data abroad using local SIM card. Imagine that wherever you travelled, you could latch on to any operator and activate a mobile subscription directly in your phone.

Travelers that use local SIM cards abroad are particularly interested in a service that would ease the process of choosing the optimal connectivity offering.

The third benefit is connected devices. Smartphones are versatile, boast larger and better screens, and become smarter by the day. With such a device in your pocket, do consumers really need mobile connectivity for other devices?

They most certainly do, and surprisingly laptops top the ranks. The main reason why consumers don't activate LTE on their smartphones are the price and lack of awareness regarding the LTE capability.

A more dangerous obstacle is the enrollment process with the operator – 57 percent of consumers with cellular-connected smartwatches mention about

how cumbersome obtaining a smartwatch subscription had been! Lifting this barrier alone could ramp up the adoption rate tremendously. For instance, 29 percent of consumers would buy a cellular-enabled smartwatch if only the enrollment process was just one click away.

And finally, Try and Buy is probably the biggest benefit of eSIM for consumers. We see it in the interest level. For example, 86 percent of respondents want to test at least one feature, which speaks to how genuinely curious we are.

But the real value of Try and Buy offerings relates to 5G. As 5G coverage extends, more and more streaming, gaming, AR/VR shopping and AR/VR learning services will emerge according to latest 5G business potential report.

However, only early adopters and digital natives will give them a try. Those following behind need to be convinced that what they are buying is worth it, which is why Try and Buy offerings are so compelling. If 54 percent of respondents are interested in 5G speeds alone, the interest for immersive video formats and AR applications can only be higher.

The opportunities with eSIM are many. Although eSIM adoption is a concern in the industry, in practice, its implementation can help enrich the relationship with consumers. From peace of mind to redeeming shopping for mobile data, eSIM is valuable to consumers. **crme**

HUAWEI

DIGITAL TRANSFORMATION IN THE ENERGY SECTOR

Alaa Elshimy, Managing Director and SVP, Huawei Enterprise Business Group, Middle East has penned an exclusive op-ed for November's edition of CNME, in which he examines the impact digitalisation is going to have on the energy industry over the next decade.



Alaa Elshimy
Managing Director and SVP, Huawei
Enterprise Business Group, Middle East

There have been regional energy companies—particularly those in the oil and gas arena—who have been embracing digitization in recent years. Their transformation is commendable, and a testament to how technology can help preserve business success. According to one whitepaper released by the World Economic Forum, digital transformation could unlock more than \$1.6 trillion in new value for the global oil and gas industry between 2017 – 2027.

The COVID-19 pandemic has served as a sharp reminder of the benefits of having a strong digital transformation strategy to ensure business continuity. This is especially the case for the oil and gas sector, which remains a pillar of many national economies in the region. Nevertheless, the oil and gas industry as a whole still has room for more digitization, a point reinforced in recent studies such as Deloitte's Digital Maturity Index.

Especially as we progress in the 4th Industrial Age, the world's demand for energy is only going to increase over the long-term, and that will require new tools being deployed in the process.

In today's environment, there is an enormous opportunity for oil and gas companies to revitalize themselves and to push for real gains as the economy recovers from the effects of COVID-19. The industry should convert its challenges into opportunities for the future – and take this moment to help revolutionize the energy sector overall. In particular, oil and gas businesses in the Middle East can now reap the benefits of investing in advanced technologies to improve operational activities, enhance their HSE plans, and bolster exploration and production.

On an operational level, leveraging emerging technologies such as AI and IoT can further enable real-time equipment and environmental conditions monitoring, while also providing transparency and greater control over processes.

That will ultimately boost efficiencies. Through deeper ICT-led automation, companies' operations can also be maintained and can continue to be productive even when dealing with a shrinking workforce.

This will prove especially beneficial for business continuity as public health



The COVID-19 pandemic has served as a sharp reminder of the benefits of having a strong digital transformation strategy to ensure business continuity.”

policies around COVID-19 evolve, aimed at protecting the health and safety of human resources.

Speaking of human resources, the oil and gas industry still very much depends on people. Using digital tools to safeguard your workforce's health and safety must remain a top priority, especially as we begin to recover from the COVID-19 pandemic.

The use of eLTE chips inside wireless gas detectors, for example, can connect personnel to the control room and the concerned HSE team members in real-time and rapidly report an alarm once a risk is detected.

An AI camera will then automatically focus on the person until he is rescued. This helps to prevent accidents and reduces losses. Through advances in IoT, we can now also make it possible to use a single, function-rich terminal for more effective inspection as well as audio and video communication. Precise tracking of personnel and assets in turn improves dispatch and command efficiencies.

In addition to operational activities and HSE, today's high-performance computing (HPC) solutions are also a strategic advantage in the race to discover oil. Mass information must be rapidly processed to accelerate decision-making.

Holistic solutions that integrate a company's hardware, systems, and cluster management, are now available to decrease the average service processing period from hours to minutes – and decrease the service processing error rate by more than half. This is increasingly valuable as companies make exploration decisions based on an enormous body of seismic and other geological survey data, whether onshore or offshore.

Given today's market challenges, nobody is under any illusions anymore. We are living in an environment where you either innovate or you disappear.

To that end, IDC and Huawei recently proposed a detailed methodology for the transformation of electric power enterprises in the whitepaper Building the Future-Ready Power Enterprise: Road to a Successful Digital Transformation. As the advance of global energy reform and digitalization develop, it will ultimately enable enterprises in the region to deliver greater business value, and at scale. **enr**

Antoine Harb*Team Leader, Middle East and Africa at Kingston*

KINGSTON

PROCESSING POWER

CNME Editor Mark Forker spoke to **Antoine Harb**, Team Leader, Middle East and Africa at Kingston in a bid to find out more about its diverse portfolio of solutions such as its NVMe, SATA and SSD technologies.

Kingston has grown to be the world's largest independent manufacturer of memory products. With global headquarters in Fountain Valley, California, Kingston employs more than 3,000 people worldwide.

Regarded as one of the "Best Companies to Work for in America" by Fortune magazine, Kingston's tenets of respect, loyalty, flexibility and integrity create an exemplary corporate culture. Kingston believes that investing in employees is essential and that each

individual employee is a vital part of the company's success.

Kingston serves an international network of distributors, resellers, retailers and OEM customers on six continents. The company also provides contract manufacturing and supply chain management services for semiconductor manufacturers and system OEMs.

In a brilliant interview, the charismatic Harb articulately conveys the unique capabilities and features of its solution offering, and why its wide range and depth of products differentiates the technology company from its market competition.

NVMe technology is known for providing superior storage, speed and compatibility, but can you elaborate on the other benefits provided by this communications interface?

One of the main benefits of NVMe SSDs is their direct connection to the CPU over the PCIe bus and usage of the NVMe Protocol, which is optimized to fully utilize the potential of a Flash based storage. This offloads the CPU and leaves more processing power for other important tasks.

In comparison to older storage technologies, NVMe reduces the storage footprint in data centers, while at the same time, a single NVMe SSD like the Kingston 2.5" U.2 DC1000M could reach the same performance as an Array of multiple SATA SSDs.



NVMe comes with the advantage of removing one of the most important bottlenecks, when it comes to the transfer of data."

NVMe has also become the standard protocol for SSDs to empower data centers and enterprise environments.

However, can you tell us why NVMe has become the technology of choice for these industry verticals?

NVMe comes with the advantage of removing one of the most important bottlenecks, when it comes to the transfer of data, allowing it to take full advantage of the high-speed storage performance of SSD and fulfilling their big data requirements.

This is particularly important considering the demands of advancing technologies such as Edge and Cloud computing, AI, ML, complex databases and financial/scientific analysis and calculations.

In order to support these technologies NVMe offers an extremely high bandwidth of over 3GB/s, allowing our SSDs to achieve predictable low-latency and high-speed I/O consistency.

Can you explain to our readers what the nuanced differences between various SSD technologies such as SATA and NVMe are?

SATA III offers a maximum theoretical transfer speed of 6Gbit/s, which is roughly equivalent to 600 MBytes/s. The SATA technology makes use of the AHCI protocol which provides only 1 command queue, holding and processing 32 commands at once and is adding to higher CPU utilization as commands get "parked" there. As such, SATA operates with a higher latency.

In comparison, NVMe uses the PCIe Bus, offering speeds of 1000MB/s per lane (PCIe 3.0) and 2000MB/s per lane (PCIe 4.0). NVMe SSDs are not restricted to a single lane either, typically using 4 lanes.

Another key difference is that NVMe is able to support 64K command queues, whilst also holding and processing 64K commands per queue.

This is what differentiates NVMe from other communication interfaces, such as AHCI or SCSI, in terms of their number of simultaneous I/O operations. Lastly, NVMe operates with much lower latency due to its direct CPU communication.

What is the flagship NVMe product in Kingston's portfolio of solutions?

That would be the DC1000M U.2 PCIe NVMe Gen3 x4. The DC1000M provides an exceptional consistent I/O delivery with sequential speeds up to 3GB/s and steady-state 4K up to 540K IOPS, allowing to manage a wide range of intense workloads.

Its Quality of Service (QoS) delivers ultra-low transactional latency for large data sets and various web-based applications, while its power loss protection (PLP) feature reduces the possibility of data loss or data corruption on ungraceful power fails.

Alongside Enterprise level SSD, Kingston Technology also offers a wide range of NVMe SSD for corporate and consumer such as the KC2500 and the A2000 SSD. **crme**

APPDYNAMICS

THE NEED FOR NETWORK VISIBILITY

David Noël, Regional Vice President, Southern Europe, Middle East & Africa at AppDynamics has penned an exclusive op-ed for November's edition of CNME, in which he explains the importance of end-to-end network visibility in order to deliver a modern digital experience.



David Noël
*Regional Vice President, Southern Europe,
Middle East & Africa at AppDynamics*

For consumers across the Middle East — an increasing number of which are digital natives — modern technology has transformed the way we live, work and play. And the challenges of home working, home schooling and social distancing in the last few months have likely made us even more reliant on the digital services that are a deeply fundamental part of everyday life. The takeaway for businesses is clear — consumers expect brand-engagement options to be wide-ranging and have no patience for issues such as confusing interfaces and high latency.

Against this backdrop, application performance management (APM) has never been more important. The modern enterprise's digital platform is now indistinguishable from its brand. But even as regional players get to grips with this axiom, they face yet more complexity... in their networks. Hybrid environments that include personal endpoints, and home and public networks are all coming into play. And an

already-beleaguered IT function has to contend with the following conundrum — how do we keep tight control on the digital experience from the employee to the customer, across all the networks within our purview, to deliver top-drawer performance from our platform?

Legacy tools aren't enough

As IT teams are asked to do more and more, we have come to realise that legacy monitoring tools such as SNMP and pcap are incapable of delivering the required visibility outside the corporate perimeter. In the COVID-accelerated digital age, we need to venture into the previously unknown and monitor networks and devices outside of our control. Only then can we optimise mean time to resolution (MTTR) on performance issues. Remember, for a B2C business, these issues mean disgusted end users switching to competitors. For B2B enterprises, they can mean violation of service-level agreements (SLAs) or service-level objectives (SLOs). None of this bodes well for profitability, for any scale of business, in any industry.

Traditional monitoring tools belong to what is now a bygone era — one of total control by IT. The cloud, Internet and SaaS platforms are now integral parts of the technology stack — a poisoned chalice thrust upon admins, who in many cases have neither the tools nor experience to handle them. Legacy IT was never meant to handle the sudden appearance of countless personal devices that daily hop from network to network.

To deliver consistent, optimal

performance, complete visibility is necessary. Keeping the new digital customer coming back for more requires that you have a comprehensive view into customer experience (CX) that includes delivery, performance, and KPIs, no matter where your users are. For example, if you have a public-network issue, you must be able to tie it to its source quickly. Was it an ISP? Was it a failure in a cloud service? Working in real time is crucial because your customers also become dissatisfied in real time. Next-day resolution is no good for the digital enterprise.

Action stations!

So, what steps can you take to address end-to-end visibility? Your corporate perimeter has been pushed outward and that means you need to see more than before to keep ahead of issues. Internet and hybrid-cloud visibility starts with ensuring that you have insight into every dependency in your delivery platforms, from distributed resources to third-party API services.

So challenging is the process of tracking down issues, that a new metric — mean-time-to-identification (MTTI) — has emerged. But accurate calculation of MTTI still calls for that all-important cross-network visibility. Broad and deep in its scope, this visibility should probe the finest levels of user experience to pinpoint issues quickly and tie them to ISPs or cloud-service failures.

We should also bear in mind that an increasing number of organisations are using SaaS

to deliver critical elements of their digital experience, presenting an effective black box to monitoring tools. SaaS experience monitoring can pull the covers back and perform granular analysis on these services. Without this level of visibility, there can be no accountability, and delivering consistent customer experiences can be problematic.

IT teams need to adopt a new way of looking at their domain. By understanding that the current lack of control can be overcome, they pave the way to reclaiming ownership of their technology stack. Regional companies that want to innovate will need to address these underlying nuances first. Somehow, there needs to be a seamless handoff between network and application operations teams for faster MTTR, all while correlating business metrics, application performance metrics, and outside-in network-related metrics to form a view that line-of-business users care about.

The benefits of end-to-end performance monitoring for your extended digital estate may be obvious. Delivery of a solution that covers all requirements and fits into your business model will require a hunt for the ideal partner. As with all business-strengthening moves, strategic partnerships will be key. But get it right and you become the puppet-master, no longer chasing cul-de-sacs, but in control of every cell of every nerve-ending within your digital domain. **crme**



To deliver consistent, optimal performance, complete visibility is necessary.”

RIVERBED

NETWORKS OF THE FUTURE

Mena Migally, Regional Vice President, META at Riverbed, has compiled an exclusive op-ed for November's edition of CNME, which examines how networks have been forced to adapt due to the increased demands that have been placed on them as a direct result of the COVID-19 pandemic.

As businesses begin to settle into a new and unpredictable normal, they are being forced into adapting their plans to maintain performance, drive productivity and support their workforce. But in adapting working practices, companies need to ensure that they are taking the right steps to build network resilience at the same time.

If they don't, businesses risk opening the door to slow running and ineffective systems, hindering employee productivity and ultimately the company's ability to successfully maintain business operations.

Work from anywhere setups are here to stay:

It is unquestionable that the pandemic has overhauled business attitudes to remote working. Organisations are now recognising that there is no longer a need for the majority of staff to work in the office, if it is not where they are most productive. In fact, recent research from Riverbed found that businesses are expecting a 50 percent increase in employees working remotely post COVID-19.

This requires a step up in network performance. In the face of a challenging economic climate, businesses need networks that can deliver productivity that is equal, if not better, than the traditional office



Mena Migally
Regional Vice President, META at Riverbed

set up. Meeting this challenge will require networks to evolve.

Networks are adapting to meet increased demand:

As a result of the rapid implementation of work from home policies, networks, limited by bandwidth and latency, struggled to maintain good speeds and levels of responsiveness. These network performance problems, in turn, negatively impacted employee productivity, as revealed in Riverbed's recent research.

To tackle the latency challenge, and unlock efficiency, businesses need to embrace emerging technology and use it as a cornerstone for evolving their networks to become more resilient. For example, introducing 5G.

Thanks to its high bandwidth connections, 5G has the potential to drive productivity by providing staff with more reliable connections, giving them smoother and quicker access to applications and downloads, and enabling them to utilise internet of things devices.

However, adding 5G, and embracing the technologies it facilitates, could inadvertently damage employee productivity through increasing the complexity of the network if not combined with effective network management.

Adopting a multi-layered approach to network management:

To guarantee employees have reliable network and application access, and can utilise capabilities such as 5G, from anywhere, businesses must invest in technology that provides end-to-end visibility. This means adopting network performance management (NPM) solutions that collect and analyse the data flowing through every application on every device.

With this holistic overview, IT teams can easily identify anomalies such as slow running applications or employees who are unable to participate in video conferencing due to limited bandwidth. Armed with this information, they will be able to quickly understand the problem and take steps to resolve it. **cnme**



5G has the potential to drive productivity by providing staff with more reliable connections."



Social network



Solutions 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

Huawei IdeaHub

New Style **Smart Office**

3-in-1 Whiteboard | Projector | Online Meeting



Scan QR code to Learn More