EXCLUSIVE TIMES

YOUR CYBER & CLOUD SPECIALIST

ISSUE 01

#VIRTUALEXN

EXCLUSIVE NETWORKS

Accelerating cloud innovations in the digital era

Nathan Clements, General Manager, Exclusive Networks – Middle East, highlights how cloud, cybersecurity and the channel can fast-track digital transformation strategies.

Today, the success or failure of any business relies on the effectiveness of their digital transformation strategies. The primary goal of any digital transformation initiative is the same for all organizations, whether small or large – to use technology to transform any service, process or experience into something more agile, flexible and cost-effective.

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

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

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

However, to illustrate cloud as just a tool to improve traditional IT, as a better way to maximize resources or as a method to cut costs, is to sell it far short. Organizations need to look at it with a more expansive and ambitious view. They have to realize that with the right vision, strategy, methodology and platforms, the cloud can be a catalyst for a pervasive digital transformation that will reverberate in the years to come.

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

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

Now more than ever, as digital transformation continues to redefine businesses, the channel needs to be in sync and enable customers to navigate the complex technology landscape. Increased cloud dependence, fragmented work environments and rising demands for cybersecurity are driving the need for a trusted advisor that will empower organizations to adapt and thrive.

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

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

We constantly evolve to stay ahead of fast-changing markets and technologies to stay relevant to our vendor and reseller partners. We have been very focused on building a portfolio with vendors who are best in their field and investing in our people because we believe only a highly committed team can drive business growth and success. We now have 22 vendors across our cloud and cybersecurity portfolios – including recently onboarded partners Vectra, Checkmarx, Quest, One Identity and Hycu – all of which deliver unique market capabilities and technologies.

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

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

> **"Now more than ever, as digital transformation continues to redefine businesses, the channel needs to be in sync and enable customers to navigate the complex technology landscape."**

Saudi Arabia: A country of boundless opportunities

Grant Taylor, General Manager, Saudi Arabia and Egypt, Exclusive Networks, delves into the company's strong presence in the Kingdom and the opportunities that await channel players.

Digital transformation plays a fundamental role in shaping the way governments and businesses across the world are adapting to new opportunities and challenges.

In Saudi Arabia, digital transformation is considered a key enabler to achieving the Kingdom's Vision 2030, which is aimed at building a digitally vibrant society as well as a diverse and thriving economy. As both public and private sectors come together to realize this objective, overall spending on ICT in the country is forecasted to reach $37 billion this year, according to global research and analyst firm IDC.

Cloud computing is a key pillar of Saudi Arabia's digital transformation strategies. In fact, in 2019, the Kingdom's Ministry of Communications and Information Technology has unveiled a 'Cloud First Policy', which mandates government and semi-governmental entities to prioritize cloud technologies when making ICT investment decisions.

As one of the leading Gulf nations when it comes embracing transformative technologies, Saudi Arabia has always been an important market for Exclusive Networks. We believe that the Kingdom is undoubtedly rife with opportunities for customers, vendors and channel players alike.
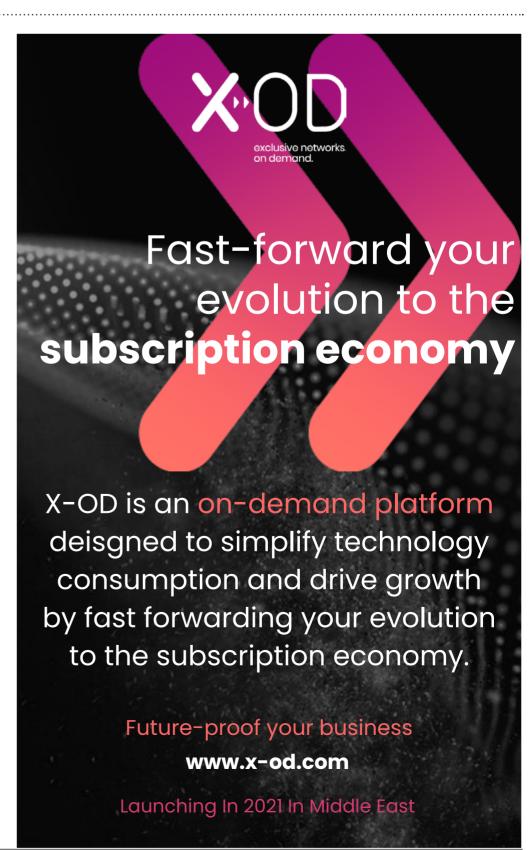
Exclusive Networks' business in Saudi Arabia has grown significantly over the last three years. We pride ourselves in having strong channel partnerships that are built on mutual trust. Today, the Kingdom is the largest market for us in terms of revenue. To further strengthen our footprint in the country, we have evolved our operations into a service-driven business, equipping our staff with the expertise to provide top-notch pre- and post-sales engagements to some of the Kingdom's largest systems integrators. We have also expanded our portfolio to include exciting and innovative solutions to strengthen our reach in this market.

In the recent past, we have seen a huge thirst for knowledge and willingness to adopt best practices with regards to the cloud among Saudi firms. That's why we believe that there are tremendous opportunities that await cloud players in this market. As a global cloud and cybersecurity value-added distributor, we recognize that for any organization the move to the cloud is an extremely personal decision. Whether they seek to implement public, private or hybrid cloud environments, this undertaking will determine the success of a company's specific current and future needs and objectives. To address this, we have increased our efforts in developing and expanding our enablement initiatives to empower our channel partners to help them better educate their customers about the cloud and its value.

We are acutely aware that any success we have had over the years is because of the dedication and trust of our vendor and channel partners. To further reiterate our commitment to this market, we will continue to improve our offerings and capabilities, deliver the highest value of service to our partners, and add new vendors to our portfolio without losing focus on the vendors that have put us where we are now. We also plan to expand our geographical reach into the Eastern and Western regions to maximize the countless prospects in the Kingdom.

As Saudi Arabia takes a giant leap towards its grand digital transformation goals, Exclusive Networks is dedicated to empowering channel partners to pave the way to the success of the next generation of digitally-enabled enterprises.

> **"We are acutely aware that any success we have had over the years is because of the dedication and trust of our vendor and channel partners."**

#VIRTUALEXN

Overcoming multi-cloud security challenges

Alain Penel, Regional Vice President – Middle East, Fortinet, sheds light on how enterprises can better manage and secure multi-cloud environments.

Cloud adoption has become an increasingly large part of CIO budgets. Today, many enterprises are already in the process of moving from an on-premises data center to a public cloud service and are planning to maintain a combination of both conventional IT and public cloud deployments.

However, while the cloud offers organizations immense business opportunities, without the right security infrastructure and operational framework in place, it presents significant challenges that can have far-reaching repercussions.

The rapid and decentralized adoption of cloud services often results in a heterogeneous set of security tools and policies that are managed in individual silos. Due to this heterogeneity of cloud deployments, there are multiple security use cases that organizations need to consider. These use cases come with security requirements such as integration of all security elements across the entire attack surface, security automation that extends across multiple clouds, cloud-specific security frameworks with centralized policy management for regulatory compliance, security that stretches across the full application life cycle, a cloud services hub for delivering security services and more.

How Fortinet is securing multi-cloud environments

Today, nearly all enterprises have embraced multi-cloud, 93% currently have a multi-cloud strategy in place. To secure multi-cloud environments, enterprises must follow three principles: native integration with all major cloud providers; a broad suite of security tools that cover the entire attack surface; and centralized management of security, including automation of workflows and threat-intelligence sharing.

Fortinet is the only company with security solutions for network, endpoint, application, data center, cloud, and access that are designed to work together as an integrated security fabric and provide true end-to-end protection.

Our purpose-built cloud security solutions collaborate with key Fortinet solutions for varying cloud deployment models, while allowing for centralized management, open API integrations, metering consumption, cloud platform orchestration, and automation.

Furthermore, Fortinet's Security Fabric reduces the need for multiple touch points and redundant policies across cloud premises and ensures governance over multi-layered security boundaries.

We also have the Fortinet Secure SD-WAN for Multi-Cloud, which is a new use case built around a FortiGate-VM next generation virtual firewall combined with a FortiManager central management console. This offering enables a unified networking and security strategy with a programmable framework to ensure consistent policies for securing and transporting traffic across multi-cloud environments.

Channel opportunities

In the wake of the COVID-19 pandemic, enterprise workers around the globe have had to adapt to full-time telework environments in order to maintain business functions. Even as we begin to transition to a new normal, the cultural impact of widespread remote work will remain. For partners, this presents an opportunity to support their customers' remote work initiatives while ensuring that they have programs in place that allow for ongoing business continuity.

To support customers who are looking to further strengthen their full-time remote workforce strategy, partners can leverage cloud components within the Security Fabric. Additionally, partners can also take advantage of Fortinet's suite of teleworker solutions to help enterprises facilitate business growth and enable them to streamline their operations during these uncertain times.

At Fortinet, we provide comprehensive training programs and certifications to ensure that our partners succeed by staying current with the latest threat and defense trends. Exclusive Networks plays a major role in supporting our channel strategy through Network Security Experts (NSE) program that enables partners to master tactical skills like configuration, troubleshooting, and monitoring, as well as planning and orchestration.

93%
of organizations already have a multi-cloud strategy in place

---

The case for behavior-based threat detection

Ammar Enaya, Regional Director – METNA, Vectra, explains how focusing on attacker behavior can improve threat detection.

Cyber-attackers today can change malware, search for unknown vulnerabilities and steal data from systems they have permission to access. But they can't change their attack behaviors as they spy, spread and steal from a victim's network.

These behaviors can be observed, giving organizations real-time visibility into active threats inside their networks. Today, the savviest organizations complement their signature-based defences with automated threat management. They stay up-to-date on prevalent attacker Tactics, Techniques and Procedures (TTPs) from evidence-based sources like the Mitre ATT&CK framework, to hypothesise possible attacks, and put appropriate controls in place.

Spotting the weak signals of an attack, hidden in the cacophony of communications, isn't easy, and requires smart, adaptive software. By combining data science, machine learning and behavioral analysis, automated threat management detects malicious behaviors inside the network, regardless of the attacker's attempt to evade signatures and whether it's an insider or outsider threat.

By focusing on attack behaviors and actions, automated threat management can identify every phase of an active attack — command and control, botnet monetization, internal reconnaissance, lateral movement and data exfiltration — without signatures or reputation lists.

Behavior-based threat detections also identify internal reconnaissance scans and port scans, Kerberos client activity, and the spread of malware inside a network. Data science models are effective at neutralising an attacker's use of domain-generation algorithms to create an endless supply of URLs for their threats.

Cybercriminals always look for new ways to conceal their attack communications, and one of the most effective — and fastest-growing — ways to do this is by hiding within another allowed protocol. For example, an attacker can use benign HTTP communication but embed coded messages in text fields, headers or other parameters in the session. By riding shotgun on an allowed protocol, the attacker can communicate without detection.

However, the detection models inherent in automated threat management can reveal these hidden tunnels by learning and analysing the timing, volume and sequencing of traffic.

It's time to jump off the signature hamster wheel, gain visibility and an understanding of the previously unknown inside your networks and cloud, and get ahead of attackers by automatically detecting and analysing the behaviors and actions that belie an attack and mitigate the threat before damage is done.

> *"By focusing on attack behaviors and actions, automated threat management can identify every phase of an active attack without signatures or reputation lists."*

Turning the gears of cloud-based threat intelligence

Ahmed Ali, VP of Sales for EMEA, Cyware, discusses how the rapid shift to cloud brought by the COVID-19 pandemic calls for increased threat intelligence.

Agility, efficiency, scalability and reduced costs. These are only some of the many reasons why organizations are moving to the cloud. The shift towards cloud is not a new phenomenon. This trend has been happening over the last several years, but the move had been gradual as organizations take their own pace based on their specific needs and strategies.

Over the recent months, as the world grapples with the challenges brought by the COVID-19 pandemic, we have witnessed that many organizations have been forced to fast-track their cloud transformation strategies to ensure business continuity amid changes in work environments.

However, the rapid move to the cloud combined with the growing number of environments make it increasingly important to ensure data security and user privacy. Unfortunately, many cloud solutions and applications that are often deployed across multiple environments are not secure by default, which makes managing an organization's Data Security Architecture a key challenge.

To address this bottleneck, security teams need to know the location of each piece of data, its movement and who is accessing it. By leveraging cloud-based threat intelligence organizations can eliminate a range of challenges across cloud platforms as it will enable them to quickly start collecting, analyzing, and operationalizing actionable insights. Cloud-based threat intelligence platforms are highly instrumental for security teams that do not have an on-premise infrastructure to support the consumption of threat intelligence. Moving forward, we can expect demands for such platforms to rise as enterprises seek ways to ensure seamless security operations in the post-pandemic world.

As a global provider of threat intelligence and cyber fusion solutions, Cyware offers a wide range of threat intelligence solutions that are available on cloud and on-premise environments.

We offer a suite of cyber fusion solutions that consists of four separate but integrated modules including a Situational Awareness Platform (CSAP), an advanced Threat Intelligence Platform (CTIX), a Cyber Fusion and Threat Response Platform (CFTR), and Security Automation and Orchestration Platform (CSOL). These solutions can be leveraged to power threat intelligence analysis and sharing, end-to-end security automation, and 360-degree threat response that leads to a faster and smarter defense. Furthermore, to help organizations with smaller teams respond to increasing cyber threats, we have also released the lightweight version of its threat intelligence platform (CTIX Lite) that is available on the cloud.

In the UAE, a recent industry study highlighted that 69% of businesses view threat intelligence as extremely important for their security strategies. In response to this growing need for such solutions, Cyware has partnered with global cloud and cybersecurity VAD Exclusive Networks to bring our innovations to the region in late 2019.

Looking ahead, we endeavour to further enable organisations across both public and private sectors to leverage threat intelligence to collaborate and develop advanced defences against evolving cyber threats.

Next level networking: Enabling the borderless enterprise

Ali Sleiman, Regional Technical Director – MEA, Infoblox, explains why organizations need to rethink their network management solutions as they embrace the cloud era.

The advancements in cloud technologies have brought a new era in networking. Organizations are increasingly realizing how to deal with rapid change and are adopting cloud deployment at a steady pace.

For most enterprises, however, it's becoming more challenging to manage increasingly complex network demands across diverse physical, virtual, and cloud infrastructure. With everything moving not just to cloud but also to multi-cloud environments, DNS, DHCP, and IP Address Management (DDI) has never been more important to businesses. Subsequently, it's also never been harder to secure, manage and control new network architectures.

Traditional on-premises network management solutions can no longer keep up. Adding to the challenge is that private, hybrid and public cloud providers lack crucial network integration, orchestration, and automation capabilities today's networks require.

As organizations go through transforming their network by adopting new technologies such as SD-WAN and SaaS applications; and adopting cloud architecture such as Amazon Web Services, Microsoft Azure and Google Cloud, the network becomes borderless and the cyber risks associated with the change is exponentially larger. This also means that the visibility into the network architecture becomes difficult, if not impossible, without the right solution in place.

Organizations need to embrace the evolution of today's network architecture and understand that in this new era, the way that we build secure networks is changing as well this is what we call 'Next Level Networking.'
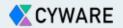
Businesses need to think differently about network security and change the way they build networks regardless of what vertical they belong to. They simply can no longer afford to think of network and security as separate fields and they need to move away from siloed solutions that lack interoperability. DNS and its ability to play a critical role in connectivity and security should be fronting the security picture and leveraged for a stronger defense.

At Infoblox, we pride ourselves in delivering next-level simplicity, security, reliability and automation to traditional networks, as well as digital transformations like SD-WAN, hybrid cloud and IoT.

In line with our vision of 'Next Level Networking', we offer solutions such as the BloxOne Platform that includes BloxOne DDI to support the branches and remote offices expansion. It is also comprised of BloxOne Threat Defense, a simplified security platform to detect and stop cyber threats. BloxOne is a cloud-native platform that not only allows our customers to scale their DDI deployment in line with the ever-evolving nature of the network architecture but also provide them with the ability to identify and alleviate network security breaches.

Looking ahead, Infoblox will continue to innovate and improve our holistic solution capabilities and by no means we will see a slowdown from that perspective. We are dedicated to further enhancing our cloud-native solution capabilities in the DDI space and cybersecurity to meet the demands of our customers and their need to scale on-premise and in the cloud.

CYWARE exabeam f5 F🔥RTINET Infoblox NUTANIX

ONE IDENTITY proofpoint Quest rubrik VECTRA

in @Exclusive Networks ME
🐦 @EXN_ME
f @EXN.ME
📷 @EXN_ME

Rubrik highlights the importance of cloud data backup

Mohammed Al Tamimi, Regional Director, Middle East, Turkey and North Africa, Rubrik, delves into how the company can help enterprises withstand cyber incidents and ensure business continuity.

Customers are increasingly adopting innovative measures to ensure business continuity in the current market landscape. We have observed accelerated cloud adoption by enterprises over the past few months to be able to deliver exceptional customer and employee experiences remotely without any operational disruptions. In such a scenario, IT leaders and organizations must pay special attention to data protection and data backup and recovery.

Rubrik, a Gartner Magic Quadrant Leader, offers pioneering data backup and recovery solutions for data in the cloud, at the edge, or on-prem. The company provides a single, policy-driven platform for data recovery, governance, compliance, and cloud mobility, which works natively in cloud services such as Amazon Web Services (AWS) and Microsoft Azure. Rubrik has local partnership with top MSPs to offer in-country private cloud for customers who want to ensure that their data remains in country, also Rubrik has strategic partnership

> **"Rubrik is a customer-first and channel-centric company. Exclusive Networks is a strategic partner for us and they play a vital role in all our initiatives in the region."**

with MSPs that offers Private cloud for the public sectors.

Regional customers can leverage unique value-adds from Rubrik solutions and drive their businesses successfully in the digital age. From ensuring data recoverability, simplifying operations, driving cloud mobility to automating workflows and achieving data control, customers can rely on Rubrik solutions for their end-to-end data management, protection and backup requirements. Rubrik stands out in the market primarily because of its strengths such as scalability, ransomware detection and remediation as well as database recovery. We can help ensure that the backbone of a customer's data center and cloud infrastructure can withstand cyber incidents such as ransomware attacks while assuring quick recovery time and business continuity after an event.

Rubrik Cloud Data Management (RCDM) is our core best-in-class backup platform and we have seen a significant increase in its adoption recently.

Rubrik is a customer-first and channel-centric company. Exclusive Networks is a strategic partner for us and they play a vital role in all our initiatives in the region. We prefer to work with focused partners such as Exclusive Networks and develop the market jointly. We are committed to growing our partners' businesses and empowering them to capitalize on market opportunities.

With a year-on-year growth of over 120 percent in the MENA region last year, Rubrik is well-positioned to support regional customers in their digital and cloud transformation journeys and address their data management and recovery challenges. Over the next few quarters, the market will us continuing to invest in the region by adding more resources and expanding our operations.

How Exabeam can advance the security posture of regional businesses

Mohammed Slim, Regional Director, Sales and Marketing, Exabeam

Remote work models have been trending over the course of this year. As organizations experience enhanced employee productivity and savings on operational costs among other benefits, these models will continue to gain in popularity and dictate the future of work.

However, this means that organizations can no longer simply have a 'tick-box culture' to show that they are compliant with the required standards and regulations. It is not at all sufficient from a security perspective, nor will organizations see the full return on investment from their SIEM solution with a compliance check mark approach.

Exabeam, a leader in the Gartner Magic Quadrant for SIEM, features a market-leading portfolio of pioneering solutions in the SIEM, UEBA and SOAR space. Our offerings - **Exabeam Advanced Analytics, Exabeam Threat Hunter and Exabeam Cloud Connectors** – help organizations track and detect any kind of abnormal activities quickly so they can take action. Our solutions significantly help to thwart malicious data breaches and shine a light on compromised credentials and insider threats through the use of machine learning and behavioural analysis. Advanced Analytics allows customers to automate the investigation of risky behavior by attackers or employees and eliminate those threats before they cause harm to the business. Coupled with Cloud Connectors, Exabeam can enable IT teams to monitor events across different cloud services and apps, including Azure, AWS, Salesforce, Office 365, Zoom and more and send them to Exabeam Advanced Analytics in an actionable format. This eliminates the need for customers to develop and maintain ad-hoc cloud services connectors.

The best part about Exabeam is that it is complementary, and not competitive, to security platforms and other SIEM solutions that customers may already have invested in. Organizations can deploy Exabeam alongside their existing security solutions and platforms to go beyond just complying with regulations and better protect their organizations, which is the goal of any SOC.

> **The best part about Exabeam is that it is complementary, and not competitive, to security platforms and other SIEM solutions that customers may already have invested in.**

Our aim continues to be to allow customers to derive more value from their existing security investments and improve their security posture with better visibility and faster response.

Reducing cyber risks with people-centric security

Emile Abou Saleh, Regional Director, Middle East and Africa, Proofpoint, discusses why a people-centric security is vital as organizations embrace the cloud amid the new normal.

If it wasn't clear before 2020, it certainly is now: people are the enterprise perimeter.

The security needs of organizations that have employees working remotely 100% of the time are different from companies with employees working from home for only once or twice a week. Remote working often means users are not protected by the same safeguards that a business has in place. It also makes it difficult for employees to verify the authenticity of emails or transaction requests with colleagues or partners.

With remote working models,

> **"Proofpoint puts people at the center of its innovation roadmap, which has allowed us to break new ground in solving core cybersecurity challenges."**

employees often need to deal with protocols, online tools, and communications that they are not familiar with. It's this lack of familiarity that threat actors will try to capitalize on.

Addressing the security challenges of remote working
Proofpoint puts people at the center of its innovation roadmap, which has allowed us to break new ground in solving core cybersecurity challenges. Our innovations provide new people-centric security and compliance blueprint for email, cloud, and information protection.

Proofpoint's solutions are built on the world's most advanced intelligence platform and stop 99% of attachment-based attacks. Our differentiator is that we look at cybersecurity with a people-centric view and focus on solutions that protect an organization's most targeted individuals.

Our channel partners and global customers can look to us to provide an unmatched level of insight into Very Attacked People (VAPs) as well as to protect them and the information they create from advanced cyberattacks and compliance risks and respond quickly when incidents occur.

Opportunities for channel players
There's no doubt that the ongoing impact of COVID-19 is taking its toll on global markets and businesses, however, our commitment to our channel partners remains unwavering.

Proofpoint is committed to its channel strategy and in fact, 100% of our new business in EMEA is indirect. We operate in close collaboration with Exclusive Networks, an established partner program with three tiers: Silver, Gold and Platinum.

Indeed, there is a significant opportunity in EMEA for Proofpoint partners, and we are investing heavily in the region and adding resources to help grow the business. We will continue to invest in the Middle East market and beyond.

The future is multi-cloud

Nasser El Abdouli, Director of Channel Sales for the Middle East, Turkey and Africa, F5, discusses the challenges faced by enterprises in the multi-cloud era.

Many enterprises today are well underway in their journey to the cloud. They are adopting cloud-based applications, platforms, and services to achieve greater flexibility and faster delivery times in an app-driven world. Currently, a heterogeneous mix of application architectures is the norm, making the era of multi-cloud the new reality.

According to F5's latest State of Application Security (SOAS) report, the EMEA region is leading the charge for per-app cloud strategies, with 88% of surveyed organizations now leveraging multicloud environments. However, it also found that many are still struggling to provide security parity across all application environments. Among the primary concerns include applying consistent security policies across all applications (30% of respondents), safeguarding against emerging threats (28%), and migrating applications between clouds and data centers (28%).

Organizations need to understand that every application is unique and serves a specific function, such as finance, sales, or production. Each will have end users that scale from less than a hundred to into the millions. And each has a different risk exposure that can span from a breach being simply embarrassing to costing the business billions of dollars' worth of damage.

That's why it is imperative to have application services that span multiple architectures and infrastructures. This will ensure consistent – and cost-effective – performance, security, and operability across the entire application portfolio.

F5's advanced app services provide the increased performance, visibility, and security that business-critical apps require.

We also deliver broad, integrated support across cloud platforms and tight integration with the tools you already use in your CI/CD pipelines. That means organizations are consistently supported, whatever their cloud journey looks like.

With F5, organizations can standardize their cloud deployments, allowing them to make a strategic investment that sets them up to be successful no matter what cloud they choose, public or private. This also enables them to deal with the complexity and diversity of services across multiple cloud providers.

Ultimately, F5 solutions can provide today's enter-

> **"F5's advanced app services provide the increased performance, visibility, and security that business-critical apps require."**

prises with the freedom to migrate existing apps with the same data path visibility, security, and management as well as build new cloud-native apps quickly.

Our robust and long-standing market capabilities, with the addition of NGINX and Shape Security, enable us to deliver the most comprehensive set of application services in the market. More importantly, we can flex to whatever cloud is needed for the job, including virtual machines, container-native, SaaS, and purpose-built hardware. Furthermore, with Exclusive Networks as one of our key partners in the region, we are confident that their strong track record and expertise will powerfully enhance our go-to-market strength.

Looking ahead, we believe that application portfolios will become even more anthropomorphic as artificial intelligence and automation become more sophisticated. We see a future where an application, like a living organism, will naturally adapt based on its environment. A combination of application services, telemetry and automation will enable it to grow, shrink, defend, and even heal itself as needed. This evolutionary shift applies to the born-in-the-cloud, digital-native organizations as well as established companies with a complex mix of traditional and modern architectures.

EXCLUSIVE NETWORKS

EXCLUSIVE *TIMES*
YOUR CYBER & CLOUD SPECIALIST

CYWARE exabeam f5 FÜRTINET.

Infoblox NUTANIX ONE IDENTITY™

proofpoint. Quest rubrik VECTRA

Accelerating IAM in the cloud

One Identity's, a Quest Software business, Sales Director for META and CEE Laurence Elbana highlights the need for robust IAM solutions as organizations accelerate their cloud journeys.

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

IAM solutions need to be built on a clear identity strategy and policy within an organization. All the identity, access and management solutions must be centralized on a platform that will not only enable customers to create users but also manage them and be able to produce the reports that can be shared with auditors and compliance teams.

This way organizations gain visibility on what users are doing and who has access to what accounts and systems. It also ensures all users are compliant and no one is above the policies set by the business.

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

To address this complexity, One Identity provides customers with the tools to synchronize both environments and create central management solutions. We have use cases for all strategies with our on-premise, cloud and hybrid identity management

solutions. This way we can cater to a specific customer's environment, be it completely cloud or on-premise or a hybrid one.

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

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

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

How Quest is modernizing digital workplaces

Amer Chebaro, General Manager and Sales Director EMEA, Emerging Markets, Quest Software, speaks about how the company enabling organizations to seamlessly move workloads to the cloud.

Please share some of the highlights at Quest over the past year.

Quest Software has been catering to customers' IT management and security requirements for over 30 years. In the past 12 months, we have evaluated our portfolio that houses over 125 products and reorganized our technology into three main pillars – manage, modernize and secure.

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

been our biggest highlight over the past year.

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

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

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

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

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

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

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

What role will Exclusive Networks play in your upcoming initiatives?

Exclusive Networks is a critical partner for us as our dedicated value-added cloud and security distributor for the region. We've been working together for about a year, and jointly we've been able to develop the Saudi, UAE and Egypt markets. They have given us access to extensive reseller networks and end-users.

Paving the way to hybrid cloud

Aaron White, Regional Sales Director - Middle East, Nutanix, spotlights why enterprises today are adopting hybrid cloud to scale up their computing capabilities.

The cloud has changed how organizations purchase and consume IT. Enterprises are continuously investing in hybrid cloud and are looking for greater interoperability between private and public clouds for all workloads, including legacy as well as cloud-native. This will push them to turn to vendors that offer platforms that can run any workload on any location without the burden of re-architecting or refactoring applications.

Enabling true hybrid cloud
As organizations re-think their cloud architectures to supplement their digital ambitions, there is a strong demand for a single platform that spans private and public clouds – that can abstract different cloud-specific intricacies – so organizations can focus on managing their traditional and modern applications irrespective of the substrates they run on.

Nutanix, as a global leader in the hyper-converged infrastructure (HCI) space, delivers a hybrid and multi-cloud platform with natively integrated networking that allows seamless application migration and license portability across all environments.

Over the past year, we have significantly added to the breadth of our platform, broadening our capabilities to address the challenges our customers tackle as they modernize their IT infrastructure and expand into multi-cloud operations.

Nutanix's offerings such as the Nutanix Prism Pro and Nutanix Calm enable IT teams to seamlessly

migrate existing applications, software licenses and operational practices between clouds without the burden of re-architecting or reworking the entire IT stack.

Empowering customers and partners
Businesses today are accelerating their digital transformation journeys by leveraging multiple clouds to satisfy their diverse enterprise computing needs. In order to support them in realizing their transformation goals, Nutanix will continue to build solutions that help customers achieve a seamless experience across multi-clouds by breaking silos and eliminating complexity.

In addition, we believe that channel partners play a significant role in empowering today's enterprises through our innovative offerings. That's why we have recently introduced Elevate, a global partner program designed to re-define the partner engagement journey. Built on an already-robust partner program, Elevate will bring together Nutanix's global partner ecosystem under one integrated architecture to deliver simplification, profitability, and an accelerated multi-product, multi-cloud roadmap towards partners' business transformation.

As a key value-added distributor for Nutanix, Exclusive Networks, with its vast network of resellers and system integrators is instrumental in driving our growth in the region. We believe that the combination of Nutanix's innovative solutions, along with the expertise of Exclusive Networks' team, will provide both partners and customers with the means to accelerate digital transformation projects in the region.

> "We enable customers to effortlessly run the full Nutanix software stack anywhere whether it's on-premise or on public clouds such as AWS or Azure."