Tackle 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 to ensure that all organizations, whether small or large, to transform or even new experience into something more agile, flexible and cost-effective.

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

Cloud plays a critical role in enabling organizations to achieve their objectives, making it an essential first step toward digital transformation.

Over the last decade, we have witnessed cloud evolve from being an industry buzzword to a key agent for business transformation. Cloud-driven initiatives have leveraged cloud computing to achieve business goals, enabling businesses to remain relevant and thriving in today’s digital ecosystem.

In a day and age where digital is redefined as an extremely personal experience, it is paramount and leveraging an expansive ecosystem is advantageous. So, a trusted-specialized cloud and cybersecurity VAR is currently evolving and improving our capabilities to enable customers and partners alike to make the most out of the digital

In the recent past, we have seen a huge shift in 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 cloud partners in this market can take advantage of. Organizations need to grow and accelerate their move to the cloud. We also continue to demonstrate our commitment to this market, our regular cloud and cybersecurity value-added distributor (VADS) Exclusive Networks is accelerating the market entry and growth for innovative cloud and cybersecurity technologies.

In the Kingdom of Saudi Arabia, we have seen that many technology players, including recently onboarded partners Vectra, Checkmarx, Quest, One Identity and Hyena – are already using cloud services and cloud technology as a way to differentiate themselves. Organizations need to take a look at it with a more expansive and ambitious view. They have realized that with the right strategy, infrastructure, and security capabilities, organizations can no longer afford to make cybersecurity a luxury. They have realized that by embracing technologies, organizations need to transform right from the outset for cybersecurity and the channel can add significant value.

In order to realize and leverage the full potential of digital transformation goals and technologies, government needs to understand how cloud and cybersecurity can add genuine value and prove the way to their customers.

In a day and age where digital is redefined as an extremely personal experience, it is paramount and leveraging an expansive ecosystem is advantageous. So, a trusted-specialized cloud and cybersecurity VAR is currently evolving and improving our capabilities to enable customers and partners alike to make the most out of the digital

In the recent past, we have seen a huge shift in 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 cloud partners in this market can take advantage of. Organizations need to grow and accelerate their move to the cloud. We also continue to demonstrate our commitment to this market, our regular cloud and cybersecurity value-added distributor (VADs) Exclusive Networks is accelerating the market entry and growth for innovative cloud and cybersecurity technologies.

In the Kingdom of Saudi Arabia, we have seen that many technology players, including recently onboarded partners Vectra, Checkmarx, Quest, One Identity and Hyena – are already using cloud services and cloud technology as a way to differentiate themselves. Organizations need to take a look at it with a more expansive and ambitious view. They have realized that with the right strategy, infrastructure, and security capabilities, organizations can no longer afford to make cybersecurity a luxury. They have realized that by embracing technologies, organizations need to transform right from the outset for cybersecurity and the channel can add significant value.
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, multi-cloud deployments can lead to significant challenges that enterprises need to face.

Fortinet is securing the cloud

Today, nearly all enterprises have embraced multi-cloud, and 90% currently have a multi-cloud strategy in place. To achieve multi-cloud environments, enterprises must first follow three principle strategy pillars integrated with all major cloud providers; a breadth of security tools that cover the entire attack surface; and centralized management and operational framework. While offering comprehensive threat intelligence, Fortinet secures the cloud.

Fortinet is the only company with security solutions for network, endpoint, cloud, and access that are designed to work together as an integrated security fabric. This enables Fortune 1000 enterprises to maintain enterprise-wide threat intelligence across five layers: threat prevention, threat detection, threat response, threat remediation, and threat correlation.

Cybercriminals always look for new ways to attack, and there is a clear correlation between an attack and the way it is being prevented and allowed to proceed. For example, an attacker can use beacons to gain access to networks and access control, but continue to exfiltrate data in text files. This can happen quickly and in the absence of any controls or alerts.

Traditional on-premises network management tools can no longer stop an attack. Adding to the challenge is that private, federal and public cloud access is crucial to modern organizational and functional integration.

For most enterprises, however, it is becoming more challenging to manage increasingly complex environments. In addition to on-premises data centers, organizations must now address emerging and distributed cloud architectures. The differences between the internet of things and the internet of industries is enormous, and not only affects the business models for traditional and cloud-native security, but also how enterprises are able to identify, authenticate and mitigate the threat before it is too late.

The capabilities of today’s network and security architecture and understanding that is new in this era, the fact that we are looking at a new model of networking, as well as what we call “Next Generation Security.” Businesses need to think differently about security network and security network. Network is a critical component of an organization, and we cannot afford to think of this internet separately from cloud services, and inability to play a critical role in cognitive and structural security. This is why the cloud must become a security force, and not just a responsibility for the business, but for our customers to scale their deployments efficiently.

Fortinet is building a comprehensive suite of teleworker solutions to meet the needs of the new normal, the cultural impact of widespread remote work will remain a significant factor, and we look forward to the opportunity to support our customers as they manage multiple cloud environments while ensuring that they have the right tools in place for allowing ongoing business continuity.

For companies that are looking to strengthen their full remote workforce strategy, partner companies can now offer high velocity point and robust solutions across cloud environments and ensure governance and multi-layered security boundaries.

In the wake of the COVID-19 pandemic, enterprises worked around the globe have had to adopt a hybrid model of work, and many enterprises 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 a significant factor, and we look forward to the opportunity to support our customers as they manage multiple cloud environments while ensuring that they have the right tools in place for allowing ongoing business continuity.

“By focusing on attacks and threats that result in breaches, without the right security infrastructure and operational framework, multi-cloud deployments can lead to significant challenges that enterprises need to face.”

The case for behavior-based threat detection

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

Cyber-attackers today can steal data from systems they change malware, search for evidence-based TTPs from evidence-based analysis, automated threat management, learning and behavioral analysis to improve threat detection.

Cyber-attackers today can steal data from systems they change malware, search for evidence-based TTPs from evidence-based analysis, automated threat management, learning and behavioral analysis to improve threat detection.

However, while the cloud offers organizations immense business opportunities, without the right security infrastructure and operational framework, multi-cloud deployments can lead to significant challenges that enterprises need to face.

By focusing on attacks and threats that result in breaches, without the right security infrastructure and operational framework, multi-cloud deployments can lead to significant challenges that enterprises need to face.

However, the detection models inherent in automated threat management can reveal these hidden tunnels by learning and analyzing the timing, volume and sequencing of data. It’s time to jump off the signature-based window, gain visibility and understanding of the previously unseen behavior of attackers and automate the response by automatically detecting and analyzing the behavior and actions that become an attack, mitigate the threat before it is too late.

The advancements in cloud technology have brought a new challenge, as data centers are increasingly dealing with rapid change and are adopting cloud deployment at a faster pace.

For most enterprises, however, it is becoming more challenging to manage increasingly complex environments. In addition to on-premises data centers, organizations must now address emerging and distributed cloud architectures. The differences between the internet of things and the internet of industries is enormous, and not only affects the business models for traditional and cloud-native security, but also how enterprises are able to identify, authenticate and mitigate the threat before it is too late.

The authors conclude that by focusing on attacks and threats that result in breaches, without the right security infrastructure and operational framework, multi-cloud deployments can lead to significant challenges that enterprises need to face.

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

“The case for behavior-based threat detection

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

Cyber-attackers today can steal data from systems they change malware, search for evidence-based TTPs from evidence-based analysis, automated threat management, learning and behavioral analysis to improve threat detection.

However, while the cloud offers organizations immense business opportunities, without the right security infrastructure and operational framework, multi-cloud deployments can lead to significant challenges that enterprises need to face.

By focusing on attacks and threats that result in breaches, without the right security infrastructure and operational framework, multi-cloud deployments can lead to significant challenges that enterprises need to face.

However, the detection models inherent in automated threat management can reveal these hidden tunnels by learning and analyzing the timing, volume and sequencing of data. It’s time to jump off the signature-based window, gain visibility and understanding of the previously unseen behavior of attackers and automate the response by automatically detecting and analyzing the behavior and actions that become an attack, mitigate the threat before it is too late.

The advancements in cloud technology have brought a new challenge, as data centers are increasingly dealing with rapid change and are adopting cloud deployment at a faster pace.

For most enterprises, however, it is becoming more challenging to manage increasingly complex environments. In addition to on-premises data centers, organizations must now address emerging and distributed cloud architectures. The differences between the internet of things and the internet of industries is enormous, and not only affects the business models for traditional and cloud-native security, but also how enterprises are able to identify, authenticate and mitigate the threat before it is too late.

The authors conclude that by focusing on attacks and threats that result in breaches, without the right security infrastructure and operational framework, multi-cloud deployments can lead to significant challenges that enterprises need to face.
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.

"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."

Many enterprises today are well under way 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 set of applications architectures is the norm, making the era of multi-cloud the new reality.

According to F5’s latest State of Application Security (SOS) report, the EMEA region is leading the charge for app cloud strategies with 88% of surveyed organizations now leveraging multi-cloud 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.

"If it’s not a lack of cloud knowledge that is stopping us, it’s the lack of understanding on how to deploy the right partner and the right services in the right way," F5’s Mohammed Al Tamimi concludes.

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

Rubrik has a dedicated channel team in the Middle East and it is growing fast with dedicated partners. Rubrik also has strong relationships with top cloud channels and provides a comprehensive set of multi-cloud capabilities. The company invests in maintaining a strong presence in cloud with the addition of NGINX and SOAR capabilities. Rubrik’s advanced app services provide the increased performance, visibility, and security that business-critical cloud applications require.

Reducing cyber risks with people-centric security

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

The future is multi-cloud

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

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

"As customers move to the cloud, they are faced with insurmountable 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 resources. It also eases on-premise users are compliant and on no one is above the policies set by the business. For some traditional workloads, on-premise IAM software and management to manage access to multiple sources. But as companies add more cloud services to their environments, managing such access becomes more complex. To address this complexity, One Identity provides customers with the tools to synthesize both environments and create central management solutions. We have use cases for all strategies with our on-prem, cloud and hybrid identity management solutions. This way we can cater to a specific customer’s environment, it’s completely cloud-native and hybrid.

Another primary use case for One Identity is the Identity Lifecycle Management, often called privileged access management or access reviewer. 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 and resources for users - for example, Office 365 and cloud access to Salesforce Cloud System and so on.

By creating an end-to-end IAM portfolio, One Identity plays an active role in helping customers address identity and access management challenges. We are continuously eliminating identity challenges and help secure customers to use active directory as they accelerate their digital transformation journeys.

One Identity offering solutions complement Exclusive Networks’ suite perfectly. As our go-to-market partner, we have been working hand in hand with Exclusive Networks to create a rich suite of customer demanders for identity access and management solutions in the region.

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 our organizations purchase and consume IT. Enterprises are constantly investing in hybrid cloud and are looking for greater interoperability between private and public clouds for all workloads, including SaaS as well as cloud-native. We will predictably turn to vendors that offer platforms that can run anywhere on any location without the burden of architecture reinventing applications.

Enabling true hybrid cloud

As organizations rethink their cloud architecture to complement their digital ambitions, there is a strong demand for a single platform that spans private and public clouds - that can abstract different cloud-specific intrinsics - so organizations can focus on the core business and not reinvent modern applications irrespective of the sub-tenants they run on.

"Enabling customers to effortlessly run Nutanix software stack anywhere - whether it’s on premise or on public clouds such as AWS or Azure.

The modernize pillar of Quest, which is around modernizing the workplace and ideal world, has been a pivot point for us as we’ve seen a big 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 milestones acquisitions have been our biggest highlight over the past year.

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 offering provides secure access, ensures the data is audited appropriately and is 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 greater benefits, more resources and increased promotions from the new program. The market will allow us to ramp-up our regional campaign and customers will have access to the cloud. We will also be releasing more innovations in the market, which will enable us to seamlessly move workloads such as Microsoft 365, SharePoint and so on, to the cloud without any operational disruptions to customers.

MAXIMIZE SYSTEM PERFORMANCE AND AUGMENT YOUR CALABILITIES

TECHNICAL TRAINING

PROFESSIONAL SERVICES

www.exclusive-networks.com

How Quest is modernizing digital workspaces

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.

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 offering provides secure access, ensures the data is audited appropriately and is 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 greater benefits, more resources and increased promotions from the new program. The market will allow us to ramp-up our regional campaign and customers will have access to the cloud. We will also be releasing more innovations in the market, which will enable us to seamlessly move workloads such as Microsoft 365, SharePoint and so on, to the cloud without any operational disruptions to customers.