UNLOCKING THE NETWORK
SECURITY OPPORTUNITY

Securing company networks has become an imperative for organisations of all sizes in the Middle East. For solution providers in the IT security sector, the challenges that organisations face in preventing advanced attacks and securing their networks can be turned into opportunity if they have the right expertise and approach in the market. *By MANDA BANDA*

> **The channel is seeing the potential for network security growth at all layers including perimeter NGFW, core firewalls, wireless security, remote access, endpoint security and email security.**
>
> SHAHNAWAZ SHEIKH, SALES & CHANNEL DIRECTOR, SONICWALL META & CEE

> **As enterprises digitise their businesses and 50bn devices come online over the next five years, cyber attackers are perpetually trying to stay one step ahead of these trends and becoming more adept at exploiting security weaknesses and avoiding detection.**
>
> SCOTT MANSON, CYBERSECURITY LEAD, MIDDLE EAST AND AFRICA, CISCO

For vendors, distributors and solution providers playing in the high risk game of cyber security, the only real constant is change. As the number of new threats continues to intensify, and the attack surface growing, organisations are equally increasing dependant on technology to drive business outcomes.

With this tidal wave of new targets and an increasingly digital workplace, exposure to network-borne threats is at an all-time high.

Effectively spotting and stopping these evolving network threats requires not just vigilance, but new approaches. It's unrealistic to expect enterprise defences to block all attacks or eliminate all vulnerabilities and that's where the expertise of savvy solution providers come in.

Pundits say rising instances of enterprise and corporate targeted cyber-attacks and threats are expected to drive the growth of Middle East cyber security market.

Analysts IDC predicts the Middle East cyber security market size is expected to grow from $11.38bn in 2017 to $22.14bn by 2022, growing at an estimated compound annual growth rate (CAGR) of 14.2%.

However, IDC noted that the high cost of innovation and IT budget constraints in organisations limit the growth of the market.

As a result of the amount of growth experienced by digital organisations, IDC stated that 76% of IT professionals say a lack of visibility is their biggest challenge in addressing network threats and challenges.

Shahnawaz Sheikh, sales and channel director, SonicWall META and CEE, said the next generation firewalls (NGFW) remain the focal point of building network security infrastructure.

Sheikh said firewalls and related technologies around it continue to remain as the critical network security solution and services need for all organisations in the region. "It doesn't matter if the same is offered as on-premise or cloud solution," he said. "In order to achieve a multi-layered security approach, such technologies continue to be in demand and we see an increase in adoption of such technologies and services."

Sheikh said the continuous investment by customers of all sizes in the areas of network security products and services is keeping the channel growth exciting and meaningful.

According to Sheikh, the channel is seeing the potential for network security growth at all layers including perimeter NGFW, core firewalls, wireless security, remote access, endpoint security and email security, continue to grow and accordingly the regional channel is making the necessary investments to meet the growing demands of these technologies from organisations of all sizes.

Jamal Al-Nabulsi, regional partner manager, META at Cylance, said the need for reliable security solutions in the Middle East is on the rise as the region has been increasingly targeted by malicious actors from all over the world.

Consequently, said Al-Nabulsi, the increasing demand from customers is driving the network security growth as every vertical in the market has been targeted in the past couple of years. "Security is top of mind on every organisations board as the consequences of a security breach are far reaching and affect a business' operation, revenue and brand," he said.

According to Al-Nabulsi, the financial crunch and regional instability has hit budgets and IT spending and the sector least affected by those factors has been security. "That's why channel partners have been developing their security capabilities to transition to this market and meet customer needs if they haven't already done so," he noted.

With network security services being offered via the cloud enterprises, SMBs and SOHO are responding positively to these services and are demanding that partners take a lead in guiding them on bespoke offerings.

Al-Nabulsi said managed services and cloud-based solutions are on the rise in the Middle East as organisations are now on the verge of adopting cloud solutions and realise the benefits of its substantial computing power, total cost of ownership and ease of

scale and management. "Security offerings are available on the cloud and hybrid solutions including network, email and endpoint, and in general adoption has been substantial in the SMB and SOHO markets," he said. "This has been followed by a rapidly growing adoption in enterprise and slowly but surely into government."

Ahmed Baig, founder and CEO of the CISO Council, a non-profit industry body with approximately 4,000 members in the Middle East, agreed with Al-Nabulsi on the growth happening in the security market and said the growing demand for more resilient infrastructure to drive the digital transformation and online presence is a key factor for better network security.

Baig said most organisations have realised that enterprise perimeter is getting wider or disappearing with the rapid adoption of mobile and other smart devices. "This requires better visibility of network traffic and behaviour demanding better network monitoring and network access controls," Baig added.

Scott Manson, cybersecurity lead, Middle East and Africa at Cisco, said cybercrime is estimated to cost business $2.1trn globally by 2019, which is four times more than the estimated cost in 2015 making security a top concern for most businesses which has now proved its seriousness by becoming a boardroom issue.

Manson said as enterprises digitise their businesses and 50bn devices come online over the next five years, cyber attackers are perpetually trying to stay one step ahead of these trends and becoming more adept at exploiting security weaknesses and avoiding detection. "To help customers address these nascent risks, Cisco together with its channel ecosystem is focused on delivering solutions across the extended network in what has been dubbed as 'Security Everywhere'," he said.

Manson said Cisco has spent over $5bn in the last three years on strategic acquisitions in the security space, including Sourcefire, OpenDNS, Lancope, Portcullis, Threat Grid and more recently Cloudlock.

He pointed out that digital transformation and cloud computing are creating huge opportunities for the channel and security is an integral component of these trends. "Security is absolutely mission critical to every organisation. As our customers

embrace this move to digital, security truly is a front and centre concern, not only in their infrastructure but as they connect more and more devices that are not connected today," he said. "Our partners help our customers to maintain a secure end-to-end environment to protect critical infrastructure, data and intellectual property."

Manson said cyber security solutions need to protect not just networks and devices, but also critical applications and data.

Amir Kanaan, managing director, Middle East and Africa at Kaspersky Lab, said trends that are driving channel partners to bring their influence to bear in the network security space range from managed services, security threats, digital transformation, hybrid and multi-cloud environments.

Kanaan said experts attribute the growing demand for managed services to the ongoing IT talent shortage in the region. "Security

> *Training is one area where partners can differentiate themselves and elevate their service offerings. Partners should invest in enabling their staff to deal with security challenges and start rolling out new technologies, like artificial intelligence.*

ZACKY VAZ, REGIONAL CHANNEL MANAGER, FORTINET

> *Security threats such as WannaCry and other ransomware threats serve as a reminder of how under-protected so many companies are. This is especially true in the Middle East, which is a frequent target for cyber attacks.*

AMIR KANAAN, MANAGING DIRECTOR, MIDDLE EAST & AFRICA, KASPERSKY LAB

threats such as WannaCry and other ransomware threats serve as a reminder of how under-protected so many companies are," he said. "This is especially true in the Middle East, which is a frequent target for attacks."

To equip channel partners with the right skills, vendors and distributors have been urged to invest in comprehensive training and certification schemes.

Kanaan explained that at Kaspersky Lab, the company believes that the partner programme is a framework that reseller organisations can use to guide and direct their investment and growth plans. "This is why Kaspersky's partner programme delivers various initiatives such as educating resellers, pre-sales assistance in key projects, post-sales support, and consulting services, which enables the channel to create an enhanced experience for their customers," he said.

Zacky Vaz, regional channel manager, Fortinet, said training is one area where partners can differentiate themselves and elevate their service offerings. "Partners should invest in enabling their staff to deal with security challenges and start implementing new technologies, like artificial intelligence, machine learning, virtual reality, operational technology and digital transformation efforts. "At Fortinet we encourage our partners to invest in expanding and perfecting their skills by enrolling for the Network Security Expert (NSE) programme, which varies in levels of expertise," he said. "We empower our distributors to deliver these trainings, and we are proud to achieve the highest number of certifications in the Middle East."

With managed security services garnering momentum in the cloud, pundits believe network security could be one area where solution providers could increase their recurring revenue streams.

Sachin Bhardwaj, director, Marketing and Business Development, eHosting DataFort, said there is migration by enterprise, SMBs as well as SOHO sectors from physical hardware security to strengthening their cloud and virtualised networks.

Bhardwaj said the market is growing rapidly where entities are looking at capitalising on the quick, precise and real time automated tools to monitor, as well as create a strong approach to mitigate threats and protect the IT infrastructure. "Today, almost all security services are now being offered via the cloud due to an explosion of cloud/SaaS services," he said.

He said the cloud security services vary from identity and access management, data loss prevention, intrusion management, security information and event management (SIEM), email and web security, business continuity and disaster recovery.

Even though the cloud has so much potential for channel partners that have made the necessary investments, challenges still persist not least because of the need for solution providers to stay abreast with the necessary skills, certifications and domain expertise.

Dipak Vagadiya, security lead, Emitac Enterprise Solutions LLC, said the challenges and resistance channel partners face when it comes to providing network security solutions, technology and services include

> *The market is growing rapidly where entities are looking at capitalising on the quick, precise and real time automated tools to monitor, as well as create a strong approach to mitigate threats and protect the IT infrastructure.*
>
> **SACHIN BHARDWAJ, DIRECTOR, MARKETING & BUSINESS DEVELOPMENT, EHOSTING DATAFORT**

undocumented networks, application data flows, lack of diagrams, documentations, customer's lack of awareness about the problem and solutions and, finding and retaining technically strong, hands on, pre-sales engineers.

Vagadiya explained that in last few years, information security product and solution vendors have played a crucial role about educating customers. "Customers have felt some information overload about the problem category they fall in and right sizing or matching the required solution," he said.

He noted that with new emerging threats and transformation to the cloud, customers are now evaluating new architectures and exploring security solutions which help protect their hybrid design. "Cloud services providers like Microsoft and Amazon are trying to bake security within their solution," he said.

Narendra Menon, managing director,

> *The challenges and resistance channel partners face when it comes to providing network security solutions, technology and services, include undocumented networks, application data flows, lack of diagrams, documentations, lack of customer's awareness about the problem and solutions and, finding and retaining technically strong, hands on, pre-sales engineers.*
>
> **DIPAK VAGADIYA, SECURITY LEAD, EMITAC ENTERPRISE SOLUTIONS LLC**

Nikon Middle East FZE, added that with technological acceleration prompting the IT security industry's development, the channel should expect opportunities to be more centred around the Internet of things (IoT) very soon. "Already, we see the effects across industries where a study by Bayt reported that almost 60% of job seekers and 65% of market leaders themselves felt the impact of a skills gap," he said. "The very first step towards addressing an issue is its acknowledgement. The distribution industry has also moved towards training, certification as a means to further develop requisite skills. We can expect to see more such steps towards the diminishing of the skills gap." ∎