MANAGED SECURITY SERVICES GAIN HOLD

As Managed Security Services (MSS) take hold in the Middle East, the enterprise sector is offering its partners significant integrated security solutions and growth opportunities. Michael Gordon investigates where the opportunities lie for resellers and the skills sets they need to succeed in the enterprise managed security services segment.

Businesses turn to providers of Managed Security Services (MSS) to alleviate the daily pressures they face related to information security, such as targeted malware, customer data theft, skills shortages and resource constraints.

These services may be conducted in-house or outsourced to a service provider that oversees a companies' network and information system security. Functions of a MSS include round-the-clock monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to emergencies. There are products available from a number of vendors to help organise and guide the procedures involved. This diverts the burden of performing the chores manually, which can be considerable, away from administrators.

Stephan Berner, CEO at Help AG, comments: "It is only in the last three years that organisations in this region have really opened up to the idea of managed services. In the market research that we at Help AG conducted in 2014, prior to launching our MSS offering, we found that concerns regarding data confidentiality, integrity and the location of data, and SLAs were among top limiting factors.

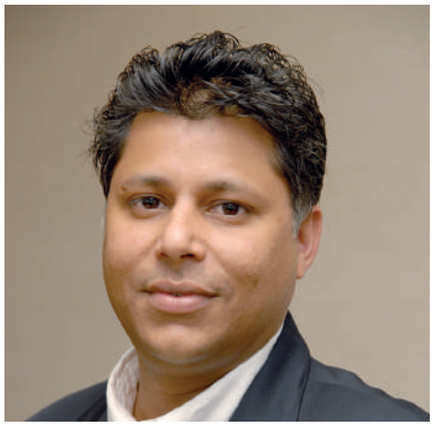
"As mature players have entered the market, with convincing offerings, a lot of these perceived risks have been addressed and I believe that the managed services market in the Middle East will evolve continuously in the years to come."

Berner added: "In 2015, we invested heavily in equipment, manpower, trainings and certifications to establish our fully functional Cyber Security Operations Centre (CSOC). Instead of partnering with third parties for this venture, which would diminish our value, we chose to implement the entire setup entirely by ourselves, thereby giving us the ability to control the whole process.

The director of Marketing and Business Development at eHosting DataFort (eHDF), Sachin Bhardwaj, said: "Added to the increasing use of cloud services, not just in the Middle East but globally, there is a growing demand and focus on the security aspects of IT infrastructure."

He added: "As we understand it, the threat landscape has been extremely volatile and sophisticated over the last few years with increasing cybersecurity attacks. Simultaneously, security solutions have also witnessed rapid advancements, with most organisations unable to cope with the speed to stay up to date. This has given rise to the growth of Managed Security Service Providers (MSSPs).

> *As mature players have entered the market, with convincing offerings, a lot of these perceived risks have been addressed and I believe that the managed services market in the Middle East will evolve continuously in the years to come.*
>
> **STEPHAN BERNER, CEO, HELP AG**



> *Added to the increasing use of cloud services, not just in the Middle East but globally, there is a growing demand and focus on the security aspects of IT infrastructure.*
>
> **SACHIN BHARDWAJ, DIRECTOR, MARKETING & BUSINESS DEVELOPMENT, EHOSTING DATAFORT**

"There is also a trend to contract the services of providers who have a more holistic approach to security. MSSPs are moving and approaching their customer needs more strategically, while having a clear vision of the future business needs."

Gartner has forecasted that 40% of all MSS contracts will be bundled with other security services and broader IT outsourcing (ITO) projects by 2020. That's double today's figure of 20%.

Muhammed Arafath, cloud solutions manager at Finesse, believes that security as a service is seen as a promising trend in the Middle East and North African (MENA) region. He said: "Customers realise they are better off trusting a security service provider who is primarily focused on evaluating threats, observing trends and compliance on a global level. It is binding on a security service provider to not just stay updated but also predict the trends, threats and compliances to stay ahead of the curve."

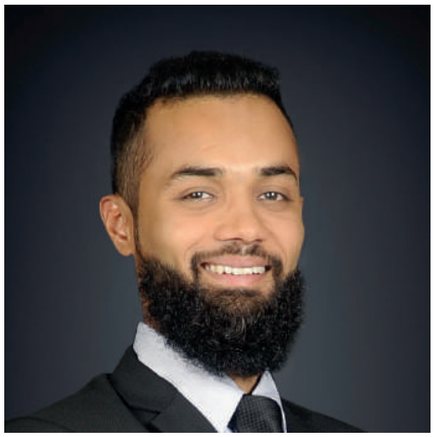
The offering

Arbor Cloud offers customers a fully managed, best-practice distributed denial-of-service (DDoS) defence service that tightly integrates on-premises and cloud-based mitigation in a single solution.

Alaa Hadi, regional director - High Growth Markets (Russia/CIS & Middle East) Arbor Networks, said: "Arbor Cloud provides in-cloud protection from advanced and high-volume DDoS attacks without interrupting access to business applications and services.

"Arbor Cloud's on-demand, multi-terabit traffic scrubbing service, staffed by Arbor's DDoS security experts, defends against volumetric DDoS attacks that are too large to be mitigated on premise. Arbor's patented Cloud Signalling capability tightly integrates on premise mitigation and cloud-based defences significantly reducing the time needed to mitigate attacks.

As a pioneer in delivering Cloud Infrastructure, Managed Hosting and Security Services in the region, eHDF's Bhardwaj said: "MSS has been part of the company's portfo-



Customers realise they are better off trusting a security service provider who is primarily focused on evaluating threats, observing trends and compliance on a global level.

MUHAMMED ARAFATH, CLOUD SOLUTIONS MANAGER, FINESSE

lio since the start of delivering Hosting Services in 2001, and ever since we have expanded the MSS portfolio to cope with the growing trends in the region."

The services and solutions eHDF offers include Real Time Threat Monitoring, Remote Managed Security Services, PCI Security Services, Advanced Threat Protection, Vulnerability Management, and Incident Response.

eHDF also recently launched a Cyber Defence Centre (CDC)/ Security Operations Center (SOC) in the UAE. It offers customers a portfolio of MSS along with Remote Managed SIEM Services. These services can be delivered either within eHDF's Data Centre, on premise at the customer's site or in the Cloud. Some of the key features include enhanced threat intelligence, custom business and technical use case development, industry vertical intelligence, regional and global threat awareness, low TCO, guaranteed SLAs and 24/7 monitoring and support.

The motivation

The prime benefit of engaging with an MSS provider is the level of technical expertise they bring. MSS providers have large pools of clients, and they invest in best-of-breed technologies that customers (especially SMBs and SMEs) would not be able to afford. MSPs also gain experience and insights from working with their large client bases which gives them a much broader understanding of the IT requirements in the region.

Unlike in-house IT teams which operate only during business hours, availability is a selling point for MSS providers as customers get 24x7 support with assured 99%+ availability, which ensures that business is always on.

Arbor's Hadi believes that cost and staffing considerations are the main drivers for managed security purchases. He said: "Teams are stretched thin at a time when their jobs have never been more difficult. Digital transformation, mobility, and Cloud are all massive transformational things which occur at once.

"The services that will be in greatest demand are those managed services that provide a differentiated skill that is beyond what the internal team has - a greater level of expertise," added Hadi.

Berner believes that the primary driver for MSS in the region is the lack of expertly qualified in-house resources, which, he argues, often results in implemented security solutions not being leveraged to the best of their potential. It is for this reason that the services that have today already proven difficult for customers to deliver in-house are things such things as 24x7 support, security monitoring and security remediation.

Berner said: "The customer interest and growth can also be linked to the cost benefits and access to expertise that MSS offer. These services help move IT budgets from intimidating CapEx to more manageable OpEx while trusting the IT infrastructure to a team of qualified experts."

The costs for both hardware and software, as well as ongoing updates and upgrades to ensure up-to-date security solutions, are something that can be circumvented by shifting away from the CAPEX model to the OPEX model that is ensured by MSSPs.

At eHDF, Bhardwaj said: "Organisations are spending a lot more to ensure competitiveness as well as to build on their future growth strategies. Aspects such as Cloud, data management and storage have been gaining traction and along with this, there is now an added focus on security. The advancement and sophistication of cyberattacks make it difficult for most organisations to keep pace. It is

Cost and staffing considerations are the main drivers for managed security purchases. The services that will be in greatest demand are those managed services that provide a differentiated skill that is beyond what the internal team has - a greater level of expertise.

ALAA HADI, REGIONAL DIRECTOR RUSSIA/CIS & MIDDLE EAST, ARBOR NETWORKS

one of the key reasons for partnering with MSSPs.

"Increasingly, across business sectors such as healthcare, finance, government, manufacturing, transportation, etc., there is a greater demand for security, and as we understand, there is a massive skills gap."

The ISACA, a non-profit information security advocacy group formerly known as the Information Systems Audit and Control Association, predicts that there will be a global shortage of two million cyber security professionals by 2019. "This has given a strong push towards the adoption of MSS," added Bhardwaj.

Regional adoption

The threat environment in the Middle East and North Africa is accelerating at a much greater pace than revenue or profits of businesses. That will keep the pressure on businesses to run efficiently, forcing them to outsource significant portions of their security, and increasingly, their entire IT infrastructure. These trends are only accelerating, so it is up to vendors to invest in their managed services, to provide top notch support, insight into performance and the attack mitigations services to fix the problem on behalf of the customer at any point of time. This addresses one of the major challenges most enterprise and government organisations are facing today which is the lack of resources and skillsets to combat the fast-changing security threat landscape 7 days a week 24 hours a day."

Naturally, the margins have to be healthy for channel partners to make a move into MSS, as the initial investment is considerable and the ongoing expenses are daunting. But like any good investment it will pay back after a few years of successful operation. "A typical channel partner will not be able to run a SOC themselves, it is a business that requires specialists rather than generalist," said Berner.

He added: "As the popularity of these services increases, I believe we will see more emphasis being placed on compliance requirements- particularly as service providers potentially handle sensitive information. It will be especially important for organisations in the public, banking and finance and even the enterprise segments to work with providers that adhere to various compliance frameworks.

"This is one of the reasons why we invested to have our MSS services certified and in compliance with the Information Security Management System ISO/IEC 27001:2013 certification."

The increasing spends on detection and response is evidently clear, and as indicated by Gartner, enterprises are transforming their security spending strategy in 2017. They are moving away from prevention-only approaches to focus more on detection and response. Worldwide spending on information security is expected to reach $90 billion in 2017, an increase of 7.6% over 2016, and to top $113 billion by 2020. Spending on enhancing detection and response capabilities is expected to be a key priority for security buyers through 2020.

At Finesse, Arafath said: "The Middle East and North Africa market understands the value of cyber security and believes that technology is not the only key element to robust security protocols but also the processes, best practices and policies implemented. The MENA market has a very significant importance on the trust factor, it is important for a client to trust the solution provider to give them this huge responsibility of managed security services. System integrators like us are in a very good position, we have our extensive client base grown over the years.

"In a market which requires specialist knowledge and very exacting quality of service guarantees partners need to do more awareness campaigns and get more familiar with the client's challenges in terms of security. The quality of trainings and end user enablement provided is very critical.

"Security is a not a one-time task, it is a commitment, therefore awareness is the key to motivation," added Arafath. ■

TYPICAL MANAGED SECURITY SERVICES

- 24x7 Security Monitoring
- Security Event Management and Incident Response
- Managed Remediation Services
- Managed Web Defence (Application Layer DDoS, Anti-Defacement, Anti-Phishing)
- Managed Web Application Firewall
- Managed Vulnerability Assessments
- Managed Endpoint Security
- Managed Endpoint Threat Detection and Response
- Managed Threat Intelligence
- Managed Forensic Analysis