

Managed security services prepare for next level

High initial investments, extended payback periods, limited skilled resources, are not inhibiting the early roll out of managed security services in the region. Key service players and vendors share their points of view. By Arun Shankar.

With the increasing use of cloud services in the Middle East and globally, there is a growing focus on the security aspects of IT infrastructure. The threat landscape has been extremely volatile and sophisticated over the last few years with increasing cybersecurity attacks. Simultaneously, security solutions have also been witnessing advancements with most organisations unable to cope with the speed to stay updated. This has given rise to the growth of managed security services.

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

As another example, Saudi Arabia is considered one of the most targeted

Many of the existing managed service providers have trouble delivering the correct service level to their customers.



► Khaled Charif, Director Technology and Innovation, NXN.



► Tusharkanti Dave, Practice Head Cyber Security Intelligence, ProVise Secure Lab.

countries and organisation of all sizes, in all industries are struggling to secure their critical assets, data, brand and reputation.

“The growth of managed services is a natural evolution of traditional ICT services, where enterprises and SMEs alike can leverage centralised analytics, reporting, decision support tools, skillsets

and expertise of a dedicated operations team. Well established technologies, such as Big Data analytics, IoT, and private, hybrid clouds are helping to fuel this growth from a technology standpoint,” points out Khaled Charif, Director Technology and Innovation, NXN.

Any business enabled by IT or exposed to the cyber world, needs protection from cyber-attacks. “Managed service providers are key enablers to bring any organisation to a higher security maturity level through a systematically designed managed security programme that consists of various cyber security initiatives spanning across years. When an organisation is in need to improve its security maturity level or improve its security posture, is when they should look out for a suitable managed security services partner,” says Tusharkanti Dave, Practice Head Cyber Security Intelligence, ProVise Secure Lab.

Power gains

So, what are the characteristics of an ideal managed security services on boarding



► Majid Khan, Manager Cybersecurity Managed Services, Help AG.



► Yasser Zeineldin, CEO eHosting DataFort.

process? Opinions differ. Continues Dave from ProVise Secure Lab, “The key drivers for any organisation to work with a managed security service provider are cost optimisation, quality outcomes, global intelligence, freedom from managing skilled resources, extended security arm, rapid incident response, event investigation, managed risk and compliance, and automating security technologies.”

“The ability to quickly leverage the benefits of a given service, with minimal upfront investment in both technology and in-house skills, is a key differentiator. The value proposition hinges around quick time-to-market, efficient commercial models, and peace of mind when it comes to operational aspects of a service’s lifecycle,” adds NXN’s Charif.

Majid Khan, Manager Cybersecurity Managed Services, Help AG, adds to this. “Two main factors driving adoption of managed security services are access to expertise and cost efficiency. Managed services help move IT budgets from intimidating capex to more manageable opex. The pay-as-you-go model lends itself to both upward and downward scalability,” says Majid Khan, Manager Cybersecurity Managed Services, Help AG.

“While a managed service provider can drive a positive impact in tackling cybersecurity needs, collaboration is the key to ensuring best results. It needs to follow a top-down approach, from the

top management downwards,” comments Yasser Zeineldin, CEO eHosting DataFort.

Enterprises that use a managed service provider can save costs by eliminating the requirement of an on-premise IT security department, getting 24x7 protection, faster deployment times and meeting compliance requirements. Primarily, the need is to

utilise existing investments made by the customer rather than replacing it, while adding additional security, multi-tenant shared services, saving additional overheads for end-user.

As an example, Saudi Arabia based, BT Al Saudia guarantees a high speed of response with lowered mean time to detect, and mean time to respond, which means less damage from threats that cannot be prevented or mitigated.

“This essentially means the key performance indicators for a security operations centre, can successfully be measured, while customers get protection for their network and IT infrastructure. Unlike traditional managed service providers, who often focus on perimeter monitoring and log collection, BT Al Saudia provides necessary business context to allow end-users to effectively assess practical implications of a risk on its business,” says Mudar Al-Ani, COO BT Al Saudia.

While some companies may opt to be niche players in managed security services, others choose to add the practice to an already existing managed services business model.

The ROI model

Achieving compliance certifications is a long-drawn process but nevertheless a necessity. Managed service providers must be consistent in their efforts in working towards these certifications. They must have the necessary procedures and people in place to ensure that they are up to date with these requirements. For the business to be profitable, there must be a significant amount of automation which can ease the



GISEC

GULF INFORMATION SECURITY EXPO & CONFERENCE
معرض ومؤتمر الخليج لأمن المعلومات

1-3 May 2018 | DUBAI WORLD TRADE CENTRE, UAE

The foremost cyber security conference & exhibition in Middle East, Africa & Asia

Security For A Connected World -
Delivered by The World's Leading Infosec Professionals

DAVID CASS
CISO, Cloud & Saas, IBM

JARKKO RAUTULA
Group CISO, IKEA Group

RUDRA MURTHY
CISO, Amazon Pay

ALEJANDRO BECERRA GONZALEZ
Group CISO, Telefónica

NG HOO MING
Deputy Chief Executive (Operations),
Cyber Security Agency Of Singapore




CHIN KIAT CHIM
CISO, DHL Express

Plus over 100 more speakers from around the world.

100s OF SESSIONS COVERING

Cyber security | Blockchain | Artificial Intelligence | IOT | Smart cities and more.

REGISTER NOW

 www.gisec.ae  +971 (4) 308 6805  gisec@dwtc.com

OFFICIAL GOVERNMENT CYBER SECURITY PARTNER



OFFICIAL DISTRIBUTION PARTNER



PREFERRED SECURITY INNOVATOR



OFFICIAL TELECOM PARTNER



OFFICIAL SECURITY SOLUTIONS PARTNER



PLATINUM SPONSORS



OFFICIAL E-CHARGING PARTNER



OFFICIAL SMART CITY PARTNER



DOMESTIC SUPPORTING PARTNER



INTERNATIONAL SUPPORTING PARTNERS



POWERED BY



PART OF



CO-LOCATED



ORGANISED BY



Achieving compliance certifications is a long-drawn process but nevertheless a necessity.



► *Mudar Al-Ani, COO BT Al Saudia.*

day-to-day navigation processes. With IT skills becoming more crucial and quite often in limited numbers as well as quality, managed service providers must be able to automate efficiently.

Managed security service providers offer real-time threat intelligence technology to identify advanced malware attacks, persistent threats, and malicious attacks. “Research driven managed security service providers, will use a threat laboratory in multiple countries to perform deep and continuous research on advanced threats. The benefit is having a managed security service provider that invests in people and technology each year into detecting and analysing global threats using threat intelligence inside a real intelligence laboratory,” says Dave from ProVise Secure Lab.

NXN provides qualified technology experts and consultants to help manage challenging security risks. “Our managed security services operational model helps entities protect and prevents against threat through effective response via collaboration between agencies with shared geographic-based information system, reduction of dispatch time and filtration of false alarms. Such a model helps customers with savings on capex and reduces opex by avoiding investment in complex technology platforms, training and management of the service, and reduces operational costs through smart management” says Charif from NXN.

While some companies may opt to be niche players in managed security services,

others choose to add the practice to an already existing managed services business model. “eHosting DataFort has been in the cloud hosting and managed infrastructure market for a long time and we have seen the huge demand for managed security services over the last few years. In our case it was a natural progression towards building a managed security services practice, to offer our customers, and to tap into the growing potential customer base,” explains eHosting DataFort’s Zeineldin.

“Given that security is a highly sensitive area of business, to build a good managed security services practice, organisations primarily must strengthen trust within existing and potential customers. This is

Once you have crossed breakeven, further increase in customers revenue, does not have proportionate increase in internal cost.

especially important, as the customer is placing critical data with the provider,” continues Zeineldin.

For BT Al Saudia, a differentiator comes with the support that is offered, since its service level agreements are aggressive. “Additionally, we are facilitating the payments on monthly and quarterly basis, assisting our customers to change over to an opex model, with the benefits of long term customer commitment and support coming from our contracts and service level agreements. This will make our managed security services model more appealing and thus increase our customer base and return from the service,” says Mudar Al-Ani at BT Al Saudia.

Help AG’s Khan points out that the first requirement for success is to be able to deliver the services locally. “This is one of the biggest factors in addressing a customer’s security concerns, but also requires a tremendous amount of investment both in developing the infrastructure and manpower. Even with this in place, as managed services are only now starting to gain traction, it would take at least a couple years before managed service providers see a full return on investment. Furthermore, many of the existing managed service providers have a lot of trouble delivering the correct service level to their customers. While the managed service providers may have a portfolio ready today, the issue is quite often inflexibility in the portfolio and services.”

Khan continues, that it is important to understand, “Managed security services requires significant initial investment in setting up the required infrastructure and getting the right people on-board to be able to run 24x7 operations, even before signing on a single customer. As this cycle is long, managed service providers should be prepared to not expect any ROI in the initial two to three years.” Once you have crossed breakeven, further increase in customers revenue, does not have proportionate increase in internal cost, thereby making this business model more interesting and profitable, Khan summarises on a positive note.

Security solutions for managed service providers

A look at vendor solutions to enable security services from managed service providers.



► *Dimitris Raekos, General Manager at ESET Middle East.*

ESET

Most of the products related to the security infrastructure for a customer can be provided through managed security services as long as there is an appropriate management platform behind them. ESET's platform for service providers includes ESET Endpoint Protection solutions for Windows, Linux, Mac, Android, iOS and in the future, it is expected to include Data Encryption and Two-Factor authentication solutions. ESET's management console integrates with the most well-known remote management and monitoring tools for partner convenience.

Managed security services are all about optimisation, it requires working with both virtual and physical environments, cloud platforms, tools to manage vulnerabilities, SIEM, IDS and RMM Tools for Remote Management. ESET's managed service provider programme offers products, daily billing and monthly invoicing to the partners.

Service providers can take advantage of volume pricing and increase profits with a tier-based pricing based on aggregation of all the clients covered. The more licenses

they sell the better unit price they get. ESET is one of the pioneers in this area and is investing resources in further developing the managed services platform.



► *Shadi Khuffash, Regional Sales Manager, Carriers and MSSPs, Fortinet.*

Fortinet

Fortinet's FortiPortal is a hosted, cloud-based, security policy management and threat analytics solutions that offers a customisable self-service portal for managed service providers customers. It provides a set of features within a multi-tenant, multi-tier management framework. This enables managed service providers to view and manage their customer networks from one single pane of glass. It also provides easy-to-deploy customer portals for self-service without having to worry about complex development or maintenance costs.

Fortinet understands that managed service providers, network service providers, systems integrators, have technology demands and support requirements. Fortinet designs its technologies to support multi-tenancy, centralised management, platform flexibility, and high-performance networks. In addition to helping managed service providers, secure customer networks more

effectively, Fortinet creates additional revenue streams, higher profit margins, and differentiation from the competition.



► *Harish Chib, Vice President, Middle East and Africa, Sophos.*

Sophos

The Sophos MSP connect is the security programme that gives managed service providers endpoint, server, firewall, mobile, encryption, web, email, and phishing simulation capabilities through a single vendor partner. Since all these products fall under the Sophos umbrella, they are integrated for protection, allowing managed service providers to offer a safer level of security.

The endpoint and network solutions that managed service providers offer to their customers in a single, security platform, also have one management dashboard, which provides a single pane of glass to see all security licenses, and all customer information, in one view.

Next-gen managed service providers must align their security strategy with vendors. Vendors, meanwhile, need to become more integrated into the managed service provider vendor ecosystem, developing and providing tools, managed



► *Shah Nawaz Sheikh, Sales and Channel Director, SonicWall META and CEE.*

service providers use to run their business and remotely monitor and manage for their customers.

SonicWall

Today's managed security services address much wider areas of security solutions, including next generation firewalls, next generation endpoint, email security, remote access solutions and wireless security to name the primary technologies. The new SecureFirst MSP Partner Programme, offers exclusive financial, enablement and support components designed to help

partners build and accelerate managed security service business.

Available to SecureFirst Silver, Gold and Platinum Partners, the SecureFirst MSSP Programme is designed to develop, enable, and support a global network of managed service provider partners. Managed service provider partners can either implement the SonicWall managed service provider blueprints by leveraging SonicWall training, technical resources and marketing assets, or jointly develop custom MSS offerings that build on the Partner's existing managed service core competencies and expertise.

Managed service providers

A look at the range of security services from top regional, managed service providers.

BT Al Saudia

The managed security services include next-generation managed SOC, managed security devices, endpoint protection, threat intelligence, vulnerability management, professional services, consultancy. BT Al Saudia brings a blend of security vendors, to provide end-to-end managed security services to customers, helping them ease their security operations. The managed security services have been designed and deployed in a well-established node supported with dedicated connectivity.

The compute building blocks consists of Cisco UCS platform to run security services and applications, such as SIEM components and vulnerability centre; server virtualisation of the security components and supporting services; storage and archiving of customer SIEM logs and events and other application data; fast and reliable IP connectivity between SOC components.

eHosting DataFort

The services and solutions include, Real Time Threat Monitoring, Remote Managed Security Services, PCI Security Services, Advanced Threat Protection, Vulnerability Management, Incident Response, amongst others. eHDF has also recently launched

a Security Operations Center in the UAE. It offers customers a portfolio of Managed Security Services along with Remote Managed SIEM Services.

These services can be delivered either within eHDF's data centre, on-premises at the end-customer site or on 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.

Help AG

The primary services are 24x7 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. Vendor partners include Splunk, Palo Alto Networks, F5 Networks, Skybox Security, Carbon Black, ThreatQuotient, Tenable, IBM, Beyond Trust and Symantec.

The infrastructure consists of domain environment, patch management, AV

and DLP solutions, multiple layers of firewalls, web applications, databases, two-factor authentication solution, web application firewalls, outbound and inbound proxies, PAM solution, Incident Response Platform, Threat Intelligence Platform, knowledge management, SIEM environment, tools for automation, and vulnerability management.

NXN

Over the last couple of years, NXN has made significant investments in building a Safe City Managed Services offering and through its integrated portfolio of technology, intelligence and insights, provide integrated digital transformation services. This includes urban safety and security, security analytics, critical infrastructure protection, for governments, real estate developers, enterprises, and small and medium customers across the GCC.

NXN has strategic partnerships with solution providers including McAfee, Vidsys, and others. NXN has built its platform with open-standards from the ground up, to integrate with different vendor technologies. The goal is not to disturb customer landscapes, but rather to connect it to the NXN open platform and augment the customer's operational capabilities with NXN managed services offering. ■