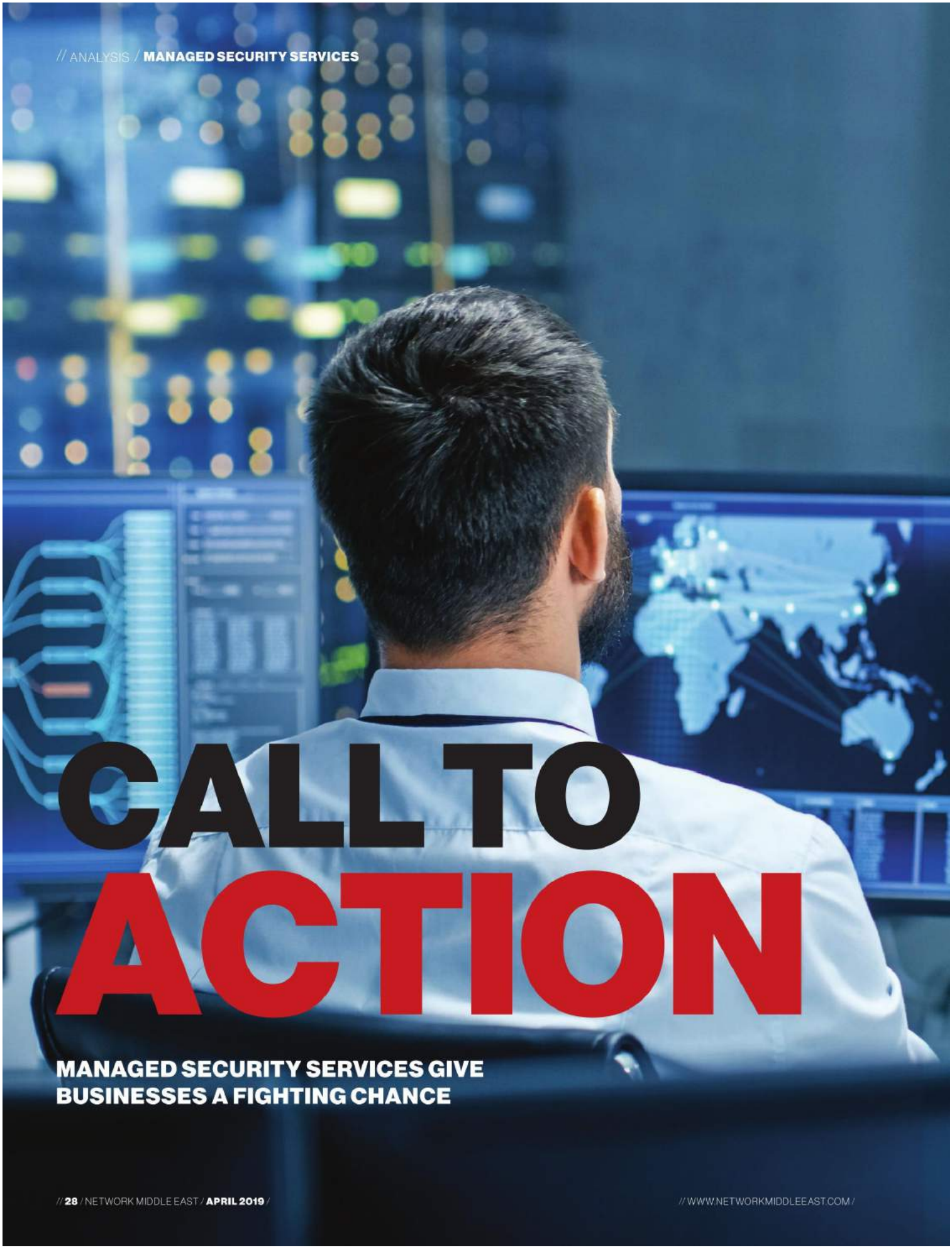


CALL TO ACTION

MANAGED SECURITY SERVICES GIVE BUSINESSES A FIGHTING CHANCE

Effective cyber defence capable of managing a myriad insider and outsider threats remains out of reach for all but the world's largest businesses.

For the rest, meagre resources have to be redirected towards securing data, affecting productivity and business growth. Fortunately, a model has emerged that enables companies to focus on running their business while experts handle their data protection needs, at a fraction of the cost: managed security services (MSS).

IT and security professionals often struggle with internal resource shortages, complex technology, worries of data theft, and the growth of mobile devices in the workplace. Therefore signing an MSSP (managed security services providers) partnership has become imperative for many organisations as now it is considered a security best-practice for companies that need better defence from the latest cyber threats, says Amir Kanaan, general manager in the Middle East, Kaspersky Lab.

In addition, MSSPs allow businesses to focus on operations while ensuring that critical assets are all properly managed and protected. Some key benefits of MSS include, access to security experts and the latest security tech, increased flexibility and lower costs, as well as improved confidentiality, compliance, and business reputation, says Kanaan.

$47.65B
MSS market size by 2023

Amit Roy, executive vice president and regional head for EMEA at Paladion, says cybersecurity is complex and requires an ever-expanding talent set and technology stack.

"Next-generation cybersecurity technology is challenging and expensive to develop, administer or manage in-house," he adds.

A global cybersecurity skills shortage has produced millions of unfilled jobs in organisations worldwide.

The right managed security service provider can provide a company the cyber defensive capabilities, tools and experienced pool of staff they require in a "turnkey" manner, backed with SLA/KPIs—without significant internal hiring, technology development or financial investment, Roy observes.

In-house IT teams, while remaining focused on daily needs, may not have the bandwidth or professional skills to tackle their cybersecurity environment, observes Sachin Bhardwaj, director, marketing & business development, at eHosting DataFort.

"Managed security service providers offer an ideal alternative that not only provides specialised skills but are in a strong position to deploy advanced security solutions and updates through their global security vendor partnerships," Bhardwaj adds.

Additionally, with strict regulations now coming into force in the region, organisations find it highly effective to outsource their security requirements to remain compliant, Bhardwaj observes.

Additionally, security comes at a high cost both to build and maintain the systems; MSSPs, therefore, enable organisations to shift from the CAPEX model to an OPEX route with predictable costs, Bhardwaj adds.

According to MarketsandMarkets, the global MSS market is expected to grow by up to $47.65 billion by 2023. Another study by Kaspersky Lab revealed that 51% of MSPs considered the essential role of cybersecurity in IT operations as the main trend to affect the MSP market over the next three to five years.

The demand for MSS is expected to increase as the threat landscape rapidly evolves, and as attacks become far more targeted, harder to predict, and complex,

> "MSS allow businesses to focus on business operations while ensuring that critical assets are protected."
>
> **AMIR KANAAN, GENERAL MANAGER, KASPERSKY LAB MIDDLE EAST**

The rapidly-changing threat landscape means the managed service providers themselves have to evolve.

Organisations in the Middle East across all sectors and sizes are major targets for advanced cyber attacks and data thefts due to their economic and geopolitical posture. And yet, most MSS providers in the Middle East only provide manual, perimeter-based, prevention-focused defences, observes Roy.

There is a need for MSS providers to

scale them up for managing deeper detection and faster response, Roy observes.

MACHINE LEARNING

The growing adoption of machine learning and automation in the MSS sector adds new impetus into MSSPs' cyber defence capabilities.

It is inevitable that MSSPs would shift towards machine learning and boosting their efforts towards strengthening their big data and artificial intelligence capabilities, observes Bhardwaj.

At its most fundamental, machine learning helps to understand and learn without set programs; at its advanced state, ML is capable of analysing behavioral patterns, advanced capabilities for threat detection and paves the way for predictive solutions for threat response.

"The sheer volume of data that is created and used today can only be structured and analysed effectively by incorporating artificial intelligence and machine learning. Intelligent machines will help in controlling network traffic and become empowered to tackle problems without human intervention. Productivity is heightened and thereby creates rooms for better ROI," he adds.

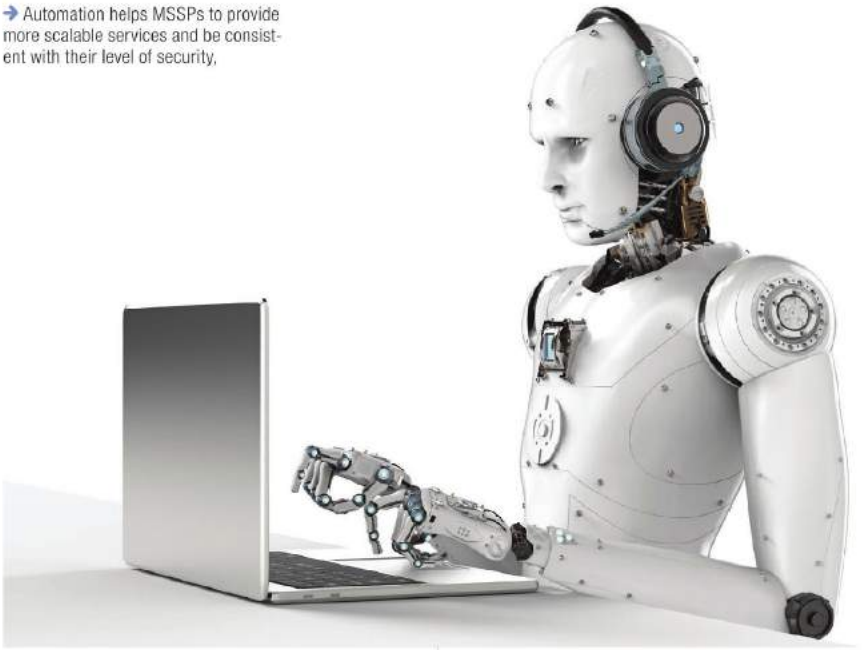
With real-time analysis driven by AI technologies, MSSPs are in a better position to attain their SLAs and garner higher customer satisfaction levels.

"Predictive analysis helps MSSPs provide real-time threat detection which significantly reduces threat risks, provides a steadier customer environment and raises the confidence levels in service quality," Bhardwaj adds.

Last year, Paladion launched a regional-first AI-driven Managed Detection and Response service. "With organisational data proliferating and cybercriminals scaling the volume and complexity of their attacks, we developed technology to automate many routine security tasks, process mass quantities of data, and identify and map new attacks in real-time which is augmented by our highly skilled cyber professionals," says Roy.

Automation helps MSSPs to provide more scalable services and be consistent with their level of security, says Kanaan. "With the growth in data, it is critical to achieve complete accuracy. This is where machine learning plays an important role – it helps to scale and manage the data," he adds.

→ Automation helps MSSPs to provide more scalable services and be consistent with their level of security.



Where the responsibility of the MSSP ends and the customer begins is a matter of constant debate.

While partnering with an MSS provider gives a unique advantage to the organisation, the risk does not 100% get transferred to the service provider. A well-structured partnership model aligning the objectives of the customer with the service provider and rolling out the key roles and responsibilities for both parties empowers the customer to achieve the most in a time-bound and measured manner.

60%
Percentage of attacks on SMBs

"While some of our clients want us to handle each of their security tasks, we do our best to adapt our security services to fit our client's unique security context and roadmap. All of this is explicitly stated in the KPI/service level agreement (SLA) we share with our clients," Roy says.

There lies a complicated relationship between customers and their security vendors within the space of cloud security as they both strive to achieve a synergetic effect towards cybersecurity, contends Kaspersky Lab's Kanaan. Before an organisation can entrust MSSPs with their data and application, it is important to define the division of responsibility – especially within a hybrid cloud environment.

"The sharing of responsibility means that it is imperative for both parties to realize that they have their own respective duties when it comes to protecting the customers' cloud data," Kanaan says.

CLOUD-MANAGED CYBERSECURITY SERVICES

The surge in cloud migration has also seen an equivalent need for cloud security. This rollout has created a great opportunity for service providers, pushing the growth of managed security services from USD 24.05 billion in 2018 to USD 47.68 billion by 2023, according to a MarketsandMarkets study.

This growth is the result of complex IT infrastructure, the adoption of IoT as well as the challenges that spring from multi-cloud usage, Bhardwaj adds.

"The volatile security landscape requires specialised skills for cloud security management. Managed security service providers can provide the services efficiently with their know-how, professional talent pool as well as domain experience, says Bhardwaj.

Cloud, however, calls for MSSPs to evolve rapidly to be in a position to tackle diverse environments, says Bhardwaj. "There is a need for MSSPs to stay abreast in the crucial areas of automation in threat detection, analysis and adaptive response to ensure that they are in a position to provide superior customer service," he adds.

The shift to the cloud is unavoidable. Hence cloud MSPs are becoming a common option. Cloud-based security portfolios allow solutions to be deployed easily and also ensures easy-to-use security management, thus increasing the cost efficiency of the business, Kanaan observes.

"Cloud service providers also offer more effective control over service levels and management. Moving to a cloud managed security service provides better security by ensuring that the data is secured across all cloud application. This also means that there will be minimum downtime in the event of a disaster," Kannan adds.

A long time ago, cybercriminals gave small and medium enterprises a wide berth, feeling perhaps they were not worth their effort. Not anymore. Smaller businesses are as much a target as large enterprises for the modern hacker-some studies show that 60% of all threats target small businesses.

Smaller companies are attractive to cybercriminals because they tend to have weaker online security, partly because they don't believe they need to invest in cybersecurity, and secondly because the high-quality cyber defence is expensive.

Managed security services, particularly delivered over the cloud, gives smaller businesses a fighting chance.

"Most MSSPs only provide manual, perimeter-based, prevention-focused defences."

AMIT ROY, EXECUTIVE VICE PRESIDENT AND REGIONAL HEAD FOR EMEA AT PALADION

Cloud allows managed security service providers (MSSP) scale managed security services, and to offer them at a cost-effective price point to organisations of any size, located anywhere in the world, says Roy

"This is very good, timely news for SMBs They are now being targeted at the same rate as large enterprises and thereby, need effective defences more than ever. Cloud-enabled MSS services give SMBs the advantage of enabling such advance services within their budget," Roy adds.

"Predictive analysis helps MSSPs provide real-time threat detection."

SACHIN BHARDWAJ, EHOSTING DATAFORT, DIRECTOR, MARKETING & BUSINESS DEVELOPMENT

Organisations now have the option to turn to cybersecurity experts to empower their own security teams so that the business can remain focus on the customer, and not putting out fires.

The world is at a tipping point as security breaches escalate. This state of affairs however presents an opportunity for regional organisations to tap into the growing capabilities of managed security services providers. MSSPs in the region are investing significantly in their operations especially in skills and automation