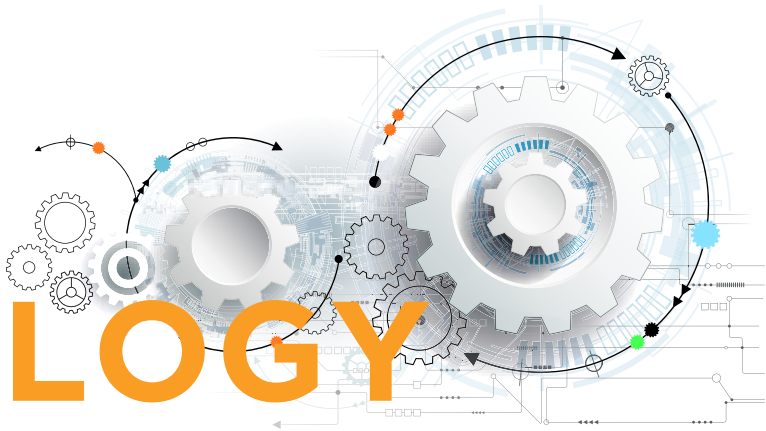
FUTURE TECHNOLOGY



The rise of the MSSPs

Rajpreet Kaur, Principal Analyst, Gartner

There are a number of factors driving the growth of the managed security services market – not least the ever-evolving cyberthreat landscape. But what are customers looking for in an MSSP? And why should they consider adopting this approach to manage their cybersecurity requirements? Industry experts at Gartner, eHosting DataFort and Help AG offer their insights to give the channel a better understanding of customer requirements and expectations.

The global managed security services market is expected to grow at a significant CAGR 6.65% during the period 2018 to 2022 as the scope and its applications are rising enormously across the globe, according to research from Radiant Insights, Inc. Managed Security Services (MSS) is termed as a systematic method to manage an administration's security needs. We spoke to industry experts about the sector in more detail to learn about some of the key factors for vendors, customers and the channel.

RAJPREET KAUR, PRINCIPAL ANALYST, GARTNER

Why should businesses and organisations consider using an MSSP?

Demand for MSSPs from enterprises and mid-sized organisations is driven primarily by a variety of factors as below:

Security staffing challenges and budget shortages: Gartner sees organisations of all sizes and geographies continuing to be challenged to attract and afford the appropriate security and risk management staff. Gartner security and risk management leaders continue to report a lack of sufficient funding and increasing budget pressures that affect their security monitoring and operations capabilities.

Better detection and response capabilities with limited staff: Organisations are embracing detection and response capabilities to complement their investments in preventive security controls. These organisations are also impacted by the increasing scarcity (or affordability) of security operations talent.

These organisations are looking for MSSPs to act as extensions of their security staff, instead of adding security head count. MSSPs can provide these services on a 24/7 basis, allowing customers to devote their often-scarce internal security resources to higher-value activities.

Evolving compliance reporting requirements: Requirements such as

As formal compliance regimes become more stringent or more pervasive, organisations are turning to external service providers to address the need to meet compliance requirements.

GDPR, NISA in the UAE, SAMA in the Kingdom of Saudi Arabia, as well as corporate governance policies, are directly driving stronger requirements for threat monitoring, identification and incident response capabilities. As formal compliance regimes become more stringent or more pervasive, organisations are turning to external service providers to address the need to meet compliance requirements.

Expansion of security event monitoring into new domains: In the Middle East, increasing attacks on the oil and gas infrastructure and the move towards the adoption of cloud services (e.g. SaaS and IaaS predominantly) is leading to concerns about the lack of visibility into these environments from a security and risk management perspective. Customers considering MSS for security services are asking about MSSP capabilities for monitoring these environments.

How should customers choose an MSSP?

- Clearly list the requirements you have
- Outline them into deliverables
- Analyse the capabilities of your in-house team
- Decide on the type of delivery model you are looking for to utilise the MSSP
- Use Gartner's RFP for MSS to design RFP or scope of work
- Discuss the type of MSS partner suitable for you as discussed before – an evolving mid-sized player, an international player or established Indian player
- If you are open to all the above, get a response from one player from each category
- Once you have checked the deliverables and pricing, make a final call on selecting the best provider for you
- Take a phased approach by starting with 24x7 monitoring and gradually upgrading/building other services

Are you able to offer any insight into the key regional players (based on Gartner research for example)?

I will classify the regional MSS players as below, with some examples:

1. **International players:** IBM, Secureworks, Symantec
2. **Indian global players:** Paladion, Wipro, Tata Communications
3. **Local telco MSS players:** Etisalat, Du, Diyar
4. **Local SI MSS players:** DarkMatter, HelpAG, Intertec

YASSER ZEINELDIN, CEO OF EHOSTING DATAFORT

In an increasingly connected world, the cybersecurity threat landscape is constantly changing. Additionally, hackers are using more sophisticated tactics. To counter this situation more organisations are turning to managed security service providers (MSSP) to tackle their cybersecurity needs to build on their security needs and help protect their networks and data.

To have an effective strategy while working with MSSPs, companies must evaluate and conduct risk assessments to ensure that get the best out of their service providers.

Primarily, organisations must ascertain the level of understanding of their business model by the MSSP who must be in a position to implement the right services and solutions. Assessment of a 360-degree approach to security must cover the whole range of technology, including hardware, software and regular updating. Other best practices include evaluation of the strength of their disaster recovery, back-up and business continuity processes.

Simultaneously, MSSPs must be appraised for their policies on risk management, skills training, processes and systems, and their compliance with industry standards and certifications. A crucial addition would be the assessment of the security skills team that will be tackling the day to day workings and ensure 24x7 availability. Lastly, the service level agreements drawn up must clearly outline the services and implementation along, and the processes and systems that will ensure quick response to any requests and issues.

However, overriding all the practices, organisations must have a top down approach where the management must be involved in their security focus and it must not be left to just the workings of the IT service provider or the internal IT department.