The managed security services ecosystem in India

Technology, threats and service providers

Driven by new security threats, new regulations and a growing universe of consumer generated data, the managed security services (MSS) marketplace is poised for accelerated growth. According to Gartner, while security and risk management (SRM) have been working 'in the shadows' all these years, they are now playing a more prominent role in IT strategy.

Also, our recent paper mentions several factors that are likely to shape the world of cybersecurity in the near-term.

These include:

- Technology evolution (DevOps, cloud)
- Digital transformation (IoT, cloud, machine learning)
- Regulation (GDPR, NIS Directive, Personal Data Protection Bill – India, consent driven laws)
- Business alignment (log collection and analysis, risk calculations)
- Critical Information Infrastructure (CII) demands
- Stronger and more proactive security protocols (readiness, integrity, availability, QA/QC)

The market for managed security services is expected to grow rapidly over the next 3–5 years. According to research by Markets & Markets, the market size for managed security services is poised to grow from USD 24 billion in 2018 to USD 48 billion in 2023.

Contents

 © Copyright NTT Ltd.

Recent incidents reiterate the need for managed security services

Last few years have been significant years in the context of cybersecurity, and were marked by prominent incidents with global impact:

- The biggest among these was 'WannaCry' a global ransomware attack that infected systems running MS Windows OS, and impacted hundreds of thousands of computers worldwide. India was one of the worst hit by WannaCry, with more than 45,000 computers affected (a former director of the Intelligence Bureau stated that the actual number of computers affected in India may by around 250,000).
- The second incident relates to the data breach at Equifax, a leading credit reporting bureau that manages the personal information (including credit card numbers) of hundreds of millions of people across the world. The data breach towards the end of 2017 led to more than 145 million accounts being compromised in USA, Canada and UK. The cost of the breach is estimated to be over USD 400 million.
- The third major cybersecurity incident of 2017 was NotPetya virus that impacted many large companies in the transportation and logistics space – such as FedEx and Maersk. The expected loss to FedEx was USD 300 million and to Maersk was USD 200 million, because of NotPetya.
- A DDOS attack of over 1Tbps on DNS service provider DYN which caused major internet platforms and services to be unavailable to large swathes of users in Europe and North America. It was unique in the use of IoT devices through the Mirai botnet and the scale and size of the attack.

We have seen a significant number of malicious cyber-events (such as data breaches, data exposure, hacks, etc.) with the discovery of Meltdown and Spectre. These are two fundamental vulnerabilities in microprocessor chips that could be exploited by hackers to access protected information. Also, earlier this year, Exactis, a US-based marketing firm that collects, manages and runs analytics on consumer data, announced that its database containing more than 340 million records (that included people's social security numbers) was left exposed on the internet. The recent hacking of credit card information from Cosmos Bank in Pune, led to fake transaction resulting in Rs. 94 crores being wiped out from the bank.

Cyberattacks are continuously growing, both in sophistication and audacity of attacks, despite companies making large investments in security tools and processes. With new threats and a fast-changing regulatory environment, the demand for cybersecurity and managed security services will continue to grow across industries. In India, the managed services market is largely unpenetrated and is likely to grow much faster than the US and Europe.

The new digital landscape is changing the nature of cyber attacks

The digital shift has been defined by unparalleled connectivity, a plethora of applications and the generation of massive amounts of data across both enterprise and consumer technology. Unfortunately, it has created many new opportunities for cybercriminals to compromise data security.

Endpoint security risks: With enterprise applications today connecting with a wide variety of applications, devices and data sources outside the firewall, systems and users are more vulnerable to viruses, spyware, ransomware, identity theft and unauthorized exposure to data.

With trends like bring your own device (BYOD), organizations face new challenges around identifying, tracking and monitoring a vast array of mobiles, tablets and other devices used by employees. Even consumer-facing applications like web portals, mobile apps, biometric devices and wearables need to be brought under a common set of security protocols. The sheer variability of consumer devices and applications makes end-point security a continuous risk. It is highly challenging for organizations to stay aligned to changing devices and platforms, and upgrade their security processes and software accordingly.

Cloud technology: In a multi-cloud world, enterprise IT environments continuously introduce new applications, devices and data across functions and geographies. Concepts such as 'hyperscale' are gaining popularity, and we see huge data farms today that hold and transact hundreds of terabytes of data. Naturally, cloud environments become a natural target for malware and other forms of cyberattacks. Cloud vendors, as well as organizations that extensively use cloud computing, need to handle several security challenges such as:

- Data loss during application migration or reengineering for the cloud.
- Vulnerabilities across integration points and APIs between cloud to cloud or on-premise applications.
- Unauthorized access to data, using malicious software (worms, ransomware, account hijacking, etc.).
- Distributed Denial of Service (D-DOS) attacks.
- Chip level vulnerabilities like Meltdown and Spectre.
- Inconsistencies in data and network encryption across different cloud platforms.

To make matters complicated, attackers are devising advanced techniques and attacks that fly under the detection capabilities of most traditional systems

 © Copyright NTT Ltd.

Fileless techniques: Cyber criminals are moving away from executable files and towards fileless approaches, which leverage authorized system utilities to launch malware attacks. Ponemon Institute estimated that more than a third of attacks on organizations will be fileless by 2018.

Since traditional security mechanisms and anti-viruses often rely on detection of malicious files, they are unable to effectively detect fileless attacks. This makes it even more critical to have a strong managed security services provider with powerful SIEM (security incident and event management) capabilities where the focus is on detection through multiple means including behavior, profiling based on machine learning and integration with threat intelligence.

Crypto-threats: At present, there are thousands of sites worldwide that are operating crypto-mining code across computers without the knowledge of their owners. Crypto-miners effectively take away significant compute power from thousands of systems, rendering them inefficient and slowing down performance.

Another type of crypto-threat is the incidence of ransomware that demands cryptocurrencies to allow users to resume access to their computers.

Social engineering: Hackers today are combining social media platforms and trust-based mechanisms to penetrate enterprise networks. The most common forms of social engineering attacks are phishing, spear-phishing, vishing and whaling. With social media becoming commonplace in workplaces, organizations today are highly susceptible to social engineering attacks.

The regulatory environment is pushing data protection

Regulatory bodies worldwide are taking active steps towards better security and consumer data protection, with have widespread implications for companies

EU is an early mover with GDPR

In May 2018, the European Union passed the General Data Protection Regulation (GDPR), giving consumers the power to consent and control the use of their personal data by enterprises. Some of the highlights of the GDPR are:

- An extended definition of personal data that now covers parameters such as cultural and social identity, in addition to demographic, health and financial information.
- Need for clear and explicit consent to collect, store and use personal data. Companies must also make it possible and easy for people to withdraw or modify consent, if they choose.
- The right to be forgotten, which means that people can ask for their data to be completely erased.
- In case of a breach, authorities must be notified within 72 hours.
- Penalties for non-compliance can go up to 20% of a company's revenues or EUR 4 million, whichever is higher.

Significant regulatory churn around data protection in India

Regulatory bodies and the central government are working together to improve data protection mechanisms through legislature. Recent moves include:

- Creation of the draft 'Personal Data Protection Bill, 2018, covering key issues such as collection, processing, quality, storage and portability. The bill borrows heavily from the GDPR, including concepts such as 'consent', 'personal critical user data' and 'right to be forgotten'.
- The bill includes terms around data localization, which means that data generated in India needs to be stored and processed in India.

With recent regulatory movement, Indian companies and cloud services providers need to make significant changes to their data architectures, technology strategies and vendor arrangements (including CSPs, MSPs, third-party data centers and hosting service providers).

Industry will need to evolve

In India we can expect a significant increase in adoption within the banking, financial services and insurance industries, which will be strongly aligned to their digital transformation and cloud migration strategies. Over time, and with greater exposure to market risks, we can also expect traditional consumer-centric industries like retail and healthcare to leverage managed security service providers (MSSPs) aggressively. The telecom industry has traditionally been ahead of the curve when it comes to data protection. However, in the digital era, even these organizations may need to partner with MSSPs to stay ahead of the cybersecurity curve. Also, as government IT departments start embarking on their cloud computing initiatives (e.g., MeghRaj by Govt. of India), MSSPs are probably the only way they can address the security needs of massive and sensitive workloads.

At the same time, increased adoption also means heightened expectations. MSSPs will need to offer more complex and comprehensive solutions that minimize the effort and risk for IT departments. To be effective, MSSPs will need to address key challenges such as:

- Staying aligned to continuously changing technology environment, including adoption of new technology stacks, devices and applications.
- Focusing on maximizing automation and service orchestration.
- Using machine learning and AI concepts to analyze large amounts of data and build powerful insights.
- Leveraging emerging technology like cloud computing and big data analytics to offer rapid scalability and availability to customers.
- Ensuring continuous availability of skilled professionals through continuous training and skill upgradation.

 © Copyright NTT Ltd.

MSSPs will see changes at various levels:

- **Network security:** Reliance on traditional firewalls and IPS will be limited to keeping the masses of threats at bay. For detecting, preventing and responding to advanced threats, MSSPs are increasingly relying on deploying network packet capture and relay technologies. These help in rewinding the complete attack scenario and provide deep dive analysis of how a breach happened. However, these are not cheap solutions. A trade-off needs to be achieved in terms of business criticality of services being monitored versus the costs of these solutions
- **End-point security:** Detecting advanced end point threats is increasingly requiring dependence on cloud for sandboxing or identification of IOCs and IOAs. However, cloud dependence also means that organizations are reluctant to send their data outside their logical span of control. MSSPs will be exploring the balance between on-premise and cloud detection capabilities that limit the type and amount of data sent to the cloud without compromising on the quality of detection.
- **Cloud security:** Most of the cloud breaches have been a factor of misconfigurations or default settings on the cloud service. MSSPs will play an important role in cloud configuration management by recommending, implementing and auditing cloud configurations for customers. Multi-cloud players with a strong security practice will be best placed to address the cloud security requirements.

Our managed security services advantage

In a highly digital environment, characterized by changing data creation and usage patterns, organizations need to continuously address vulnerabilities in their IT environment, while ensuring proactive remediation.

As a comprehensive provider of managed security services, we can help your IT department to be more effective by:

- Taking up the entire responsibility of threat detection and remediation, with minimal intervention required by IT teams.
- Providing a 24/7 Security Operations Center (SOC) that ensures real-time response and quick remediation.
- Driving a highly effective Managed Service model with options to provide own tools and leverage your existing tools.
- Leverage a strong expertise in systems, networks, database, middleware to provide you with comprehensive support.

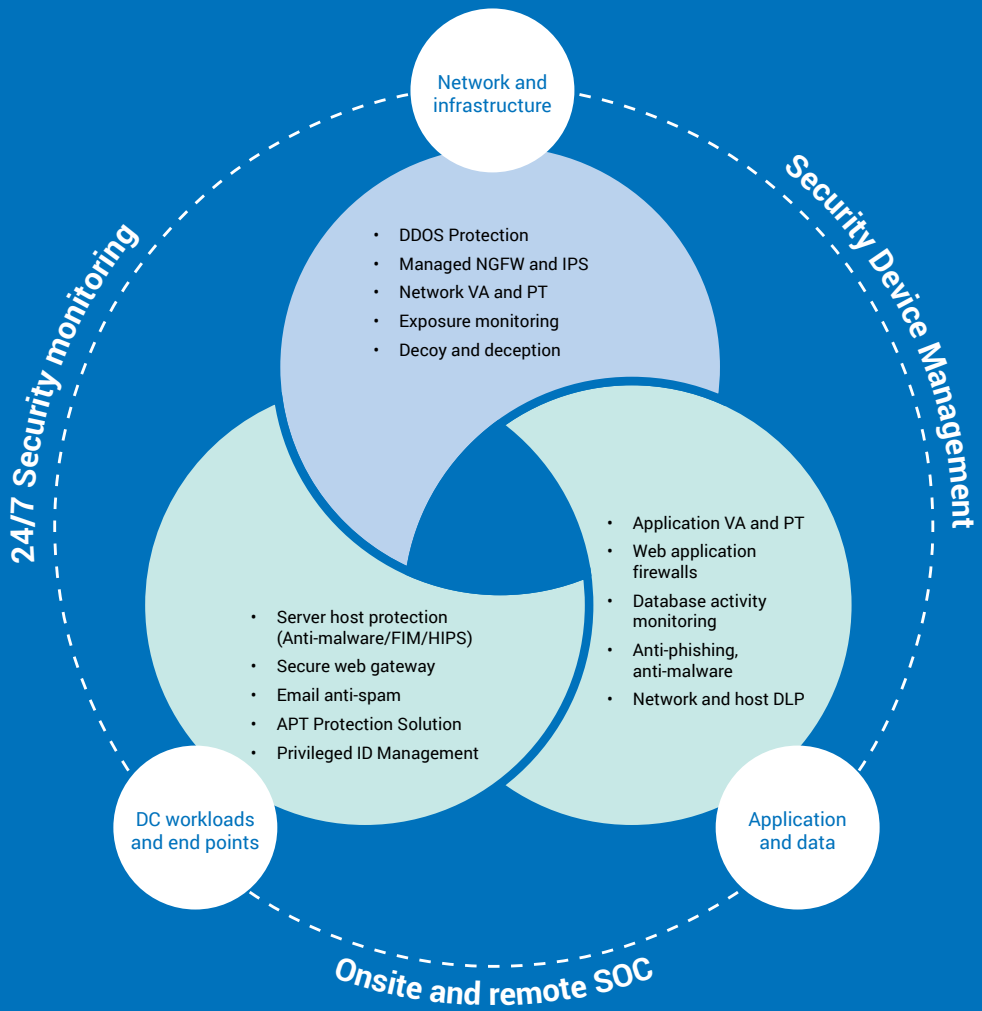
Our MSS helps minimize risks, protect critical information and effectively reduce the cost and complexity of your security infrastructure. With an end-to-end suite of fully managed services, we give you a consolidated view of your security environment, within as well as outside the enterprise perimeter. Our capabilities span across online platform-based tools as well as on-premises solutions, providing you a comprehensive set of security options for enterprises, covering:

- 24/7 security monitoring with SIEM and analytics.
- Managed web application firewall.
- Managed DDOS mitigation.
- Managed intrusion prevention.
- Exposure monitoring.
- End point threat detection and response.
- Data leakage prevention.
- Web and email threat prevention.
- Anti-phishing and antimalware protection.
- Privilege ID management.

Our MSS teams help you architect, deploy and operate security solutions leveraging best-of-breed technologies while integrating your existing security investments. We bring a significant knowledgebase of security controls, policies, best practices and frameworks that are deployed out of the box for you.

 © Copyright NTT Ltd.

Appendix



Built with the experience and expertise of more than two decades, our services have been acknowledged by some of the IT Industry's leading authorities.

CIO Choice Awards 2019

Hybrid Multi Cloud, Hyper-Scale Data Center, SD-WAN Services, Managed Cyber Threat Detection service

Economic Times

Iconic Brand of India, 2018

Frost & Sullivan India ICT Award 2018

Managed Hybrid Cloud Service Provider of the Year

DCD Awards

Energy Efficiency Improver's Award 2018

 © Copyright NTT Ltd.


NTT