THE MANAGED SECURITY SERVICES (MSS) ECOSYSTEM

TECHNOLOGY, THREATS AND SERVICE PROVIDERS

Driven by new security threats, new regulations and a growing universe of consumer generated data, the Managed Security Services 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, a recent paper by NTT Security mentions a number of factors that are likely to shape the world of cybersecurity in the near-term, such as –

> 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 bn in 2018 to USD 48 bn in 2023.

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 lakhs of computers worldwide. India, in fact 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 2.5 lakhs).

> 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 MN and to Maersk was USD 200 MN, 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 - 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. Closer to home, 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.

We see that despite companies making large investments in security tools and processes, cyberattacks are continuously growing – both in sophistication and audacity of attacks. 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 – defined by unparalleled connectivity, a plethora of applications and the generation of massive amounts of data - across both enterprise and consumer technology, 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 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, wearables, etc. 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 highly multi-cloud world, enterprise IT environments continuously introduce new applications, devices and data, seamlessly, 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 a number of security challenges such as:

  > Data loss during application migration or reengineering for the cloud

  > Vulnerabilities across integration points and APIs between cloud – cloud, or cloud – 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 and infrastructure

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

- > **Fileless Techniques:** More and more cyber criminals are moving away from executable files and towards fileless approaches, which leverages authorised system utilities to launch malware attacks. Ponemon Institute estimates that more than a third of attacks on organizations will be fileless in 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 behaviour, profiling based on machine learning, integration with threat intelligence etc.

- > **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. Some of the recent regulatory movement would have widespread implications for companies.

EU is an Early Mover with GDPR
In May 2018, the European Union flagged off the General Data Protection Regulation (GDPR), giving consumers the power to consent and control the use of their personal data by enterprises. Highlights of 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 upto 20% of a company's revenues or € 4 MN, 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 GDPR – type 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 me 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 (with CSPs, MSPs, third-party data centers and hosting service providers).

INDUSTRY WILL NEED TO EVOLVE

Particularly 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 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. Managed Security Service Providers (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

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 re-winding the complete attack scenario and provide deep dive analysis of how a breach happened. However, these are not cheap solutions and 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 organisations are squirmish about sending their data outside their logical span of control. MSSPs will be innovating with balancing the on-premise vs 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 such as Netmagic with a strong security practice will be best placed to address the cloud security requirements.

THE NETMAGIC MSS 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. A comprehensive provider of Managed Security Services like Netmagic enables IT departments 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 customer's existing tools

› Leverage a strong expertise in systems, networks, database, middleware to provide a comprehensive support to customer
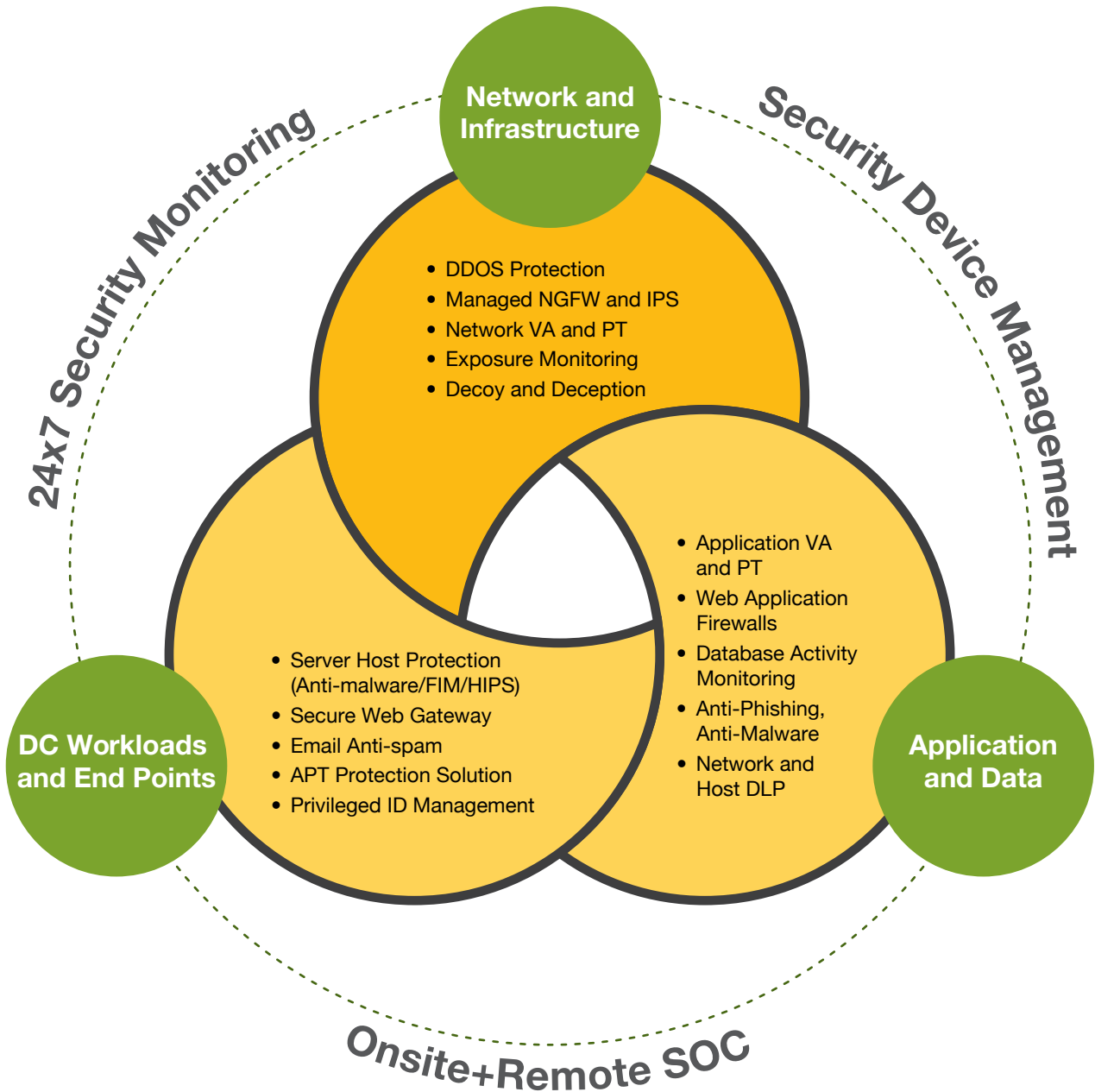
Netmagic's MSS helps minimize risks, protect critical information and effectively reduce the cost and complexity of your security infrastructure. With an end-to-end suite of fully managed services, MSS gives you a consolidated view of your security environment, within as well as outside the enterprise perimeter. Our capabilities span across online platform-based tools as-well-as on-premise solutions, providing you a comprehensive set of security options for enterprises, covering:

› 24X7 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 & Antimalware protection

› Privilege ID management

Our MSS teams help customers architect, deploy and operate security solutions leveraging best-of-breed technologies while integrating customer's existing security investments. Netmagic brings to the table significant knowledgebase of security controls, policies, best practices and frameworks that are deployed out of the box for customers.

APPENDIX

Comprehensive Approach to Security

24x7 Security Monitoring

Security Device Management

Network and Infrastructure

- DDOS Protection
- Managed NGFW and IPS
- Network VA and PT
- Exposure Monitoring
- Decoy and Deception

DC Workloads and End Points

- Server Host Protection (Anti-malware/FIM/HIPS)
- Secure Web Gateway
- Email Anti-spam
- APT Protection Solution
- Privileged ID Management

Application and Data

- Application VA and PT
- Web Application Firewalls
- Database Activity Monitoring
- Anti-Phishing, Anti-Malware
- Network and Host DLP

Onsite+Remote SOC

About Netmagic

Netmagic, a wholly-owned subsidiary of NTT Communications, is India's leading Managed Hosting and Multi-Cloud Hybrid IT solution provider with 9 carrier-neutral, state-of-the-art hyperscale and high-density data centers, and serving more than 2000 enterprises globally. Headquartered in Mumbai, Netmagic also delivers Remote Infrastructure Management (RIM) services to various Enterprise customers globally including NTT Communications' customers across the Americas, Europe and the Asia-Pacific region. The Company was the first in India to launch multiple services including Cloud Computing, Managed Security, Disaster Recovery-as-a-Service (DRaaS) and Software-Defined Storage. NTT Communications and Netmagic have been ranked 3rd and 5th respectively in Asia among the top global data center operators by Cloudscene in their Q1 & Q2 2017 Leaderboard reports. This effectively makes Netmagic the #1 data center service provider in India. Netmagic has been recognized with 3 awards at the CIO Choice Award 2018 and Frost & Sullivan India ICT Awards 2018.

To learn more, visit us at: www.netmagicsolutions.com.

About NTT Communications Corporation

NTT Communications solves the world's technology challenges by helping enterprises overcome complexity and risk in their ICT environments with managed IT infrastructure solutions. These solutions are backed by our worldwide infrastructure, including industry leading, global tier-1 public and private networks reaching over 190 countries/regions, and more than 400,000m2 of the world's most advanced data center facilities. Our global professional services teams provide consultation and architecture for the resiliency and security required for your business success, and our scale and global capabilities are unsurpassed. Combined with NTT Data, NTT Security, NTT DOCOMO and Dimension Data, we are the NTT Group.

www.ntt.com | Twitter@NTT Com | Facebook@NTT Com | LinkedIn@NTT Com

---

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

Talk to us today to know how the experts in our Managed Security Services team can help you.

1800 103 3130

marketing@netmagicsolutions.com | www.netmagicsolutions.com | www.in.ntt.com

@netmagic   @Netmagic   Netmagic

Netmagic (An NTT Communications Company)
Lighthall 'C' Wing, Hiranandani Business Park, Saki Vihar Road, Chandivali, Mumbai - 400 072.