FROST & SULLIVAN

netmagic | NTT

EMBRACING NEXT GENERATION SECURITY FOR A **SECURED DIGITAL LANDSCAPE**

Leveraging a Security Architecture that Observes, Orients, Decides, and Acts intelligently on a Threat Stimulus

As enterprises travel the Digital Transformation journey, it is important that the fundamental cyber-security strategies are re-looked at once again

SECURITY IN TODAY'S **DIGITAL LANDSCAPE**

It's an open secret that Digital Technologies have started to transform businesses globally. Enterprises have shown considerable interest towards adoption of technology concepts like Cloud, IoT, BYOD and Connected Workplace that play a pivotal role in the transformation process. While this technological metamorphosis is indeed healthy for an organisation, chief security officers realize the seriousness around security in the digital landscape.

Today, the complexity around security has increased noticeably. Security threats have increased multifold and enterprises struggle dealing with security threats. The cyber threats have moved beyond the conventional network perimeter, making it imperative to protect the infrastructure, application, endpoint and cloud resources.

If stock of the situation is taken, it would be inferred that the trouble around security is mainly due to threat management and security operations. Enterprises have to adopt newer technologies that boost productivity and employee efficiency; however they face security challenges in syncing existing security frameworks with these disruptive technologies. On a broader perspective, this challenge is due to three main aspects of threat management:

1. **The Rise of undetected Polymorphic Attacks**
2. **Introduction of Integrated Technology Processes within enterprises**
3. **Limited Visibility into Digital Infrastructure**

> *Around 50% of Indian CXOs believe Security to be a critical component of Digital Transformation*

CHALLENGES OF TRADITIONAL SECURITY

With increasing sophistication of the threat actors, the volume and severity of attacks have increased. Everyday existing security tools are being tested in their capabilities to stop an attack. While some of these security solutions prevent a known cyber threat, several others pass through the network unnoticed. To protect against this changing threat landscape, enterprises need to look at security in a new way.

Maximizing security in the enterprise ecosystem requires action that is difficult yet highly important. Enterprises need to take an intelligence based approach that is proactive and has the ability to detect unknown threats. Traditional security would not be able to provide the right investigation capability, detection, and incident response or threat mitigation. Today, threat mitigation is related to cognitive learning that analyzes user behavior and organizational patterns. Legacy security systems that use manual processes cannot keep pace with the changing threat landscape. Hence, the need for next-generation cyber security measures meant for today's threat landscape.

> *More than 60% of Indian Enterprises are either not sure or have experienced a security incident in the last 1 year*

EXHIBIT 1: DRAWBACK OF FIRST GENERATION SECURITY TOOLS

Provides only Reactive Security

Traditionally, security solutions have been reactive. A reactive solution works on the principal of acting only when damage has been registered. However, with the growing number of non-signature bases attacks, security solutions need to understand the nature of threats, analyze malware behavior and hence provide proactive security. Proactive Security functions when an attack is yet to happen and alarms the agent of a possible security breach.

Lack of Incident Response functionality

The motive behind Incident Response is to handle the situation after a cyber breach. It tries to limit damage and minimize recovery time and cost. Incident Response requires analyzing data logs collected from multiple sources and connecting each of the dots to recreate the breach. Traditional security tools fail to provide the level of intelligence required to pinpoint the correlation between events and develop a response mechanism.

Not built to comply with Industry Mandates

As cyber attacks have become rampant across industries, regulatory bodies have come up with industry mandates (e.g. BFSI, Healthcare, Power sector, etc.). These regulatory bodies need data to be monitored for auditing and forensics purposes. However, traditional security tools are not built to provide a single unified window to monitor security threats across multiple devices. Hence, enterprises need to have security products that offer easy integration with industry regulations.

No Investigation or Breach Assessment Capability

First generation security solutions do not have the capability to conduct forensic investigations into incidents. An advanced security tool brings in the context to the attack: the origin of the attack, modus operandi, compromised assets, damage caused and timeline to the attack. This in a nutshell provides forensic capabilities to the solution.

Source: Frost & Sullivan

A JOURNEY TOWARD EMBRACING **NEXT GENERATION SECURITY**

The Narrative

Before we look into the nitty-gritties of Next Generation Security posture, it is important that we understand the global megatrends that affect the positive uptake of security solutions. The 21st Century saw large data breaches that made headlines and kept CISOs anxious. As per CSO Online, the global magazine for cyber security, Yahoo lost $3 Bn. in 2013; Marriott $500 Mn in 2018; Equifax $143 Mn. in 2017; and eBay $145 Mn. in 2014. All these attacks affected millions of customers as user accounts were hacked and compromised. Not that these companies did not use security technologies; just that they did not have the right set of security products or processes that could stop advanced malware, vulnerability or data theft.

The Global Megatrend in Security has put lot of pressure on Chief Executives to protect Enterprise Assets and Customer Data. Security is no more considered the responsibility of only the CIO or CISO but every stakeholder in the business. Newer designations like Chief Risk Officer, Privacy Officer and Governance Heads are being crafted to increase focus around security. Industry mandates in Banking, Insurance, Healthcare and Power are being introduced to pay attention to the escalated security threats across these sectors. The conversation within boardrooms has shifted from threat prevention to threat identification, prevention and mitigation. To put everything in box, the journey toward next generation security has started.

EXHIBIT 2: GLOBAL MEGA-TRENDS, FROM THE CYBER SECURITY PERSPECTIVE

Source: Frost & Sullivan

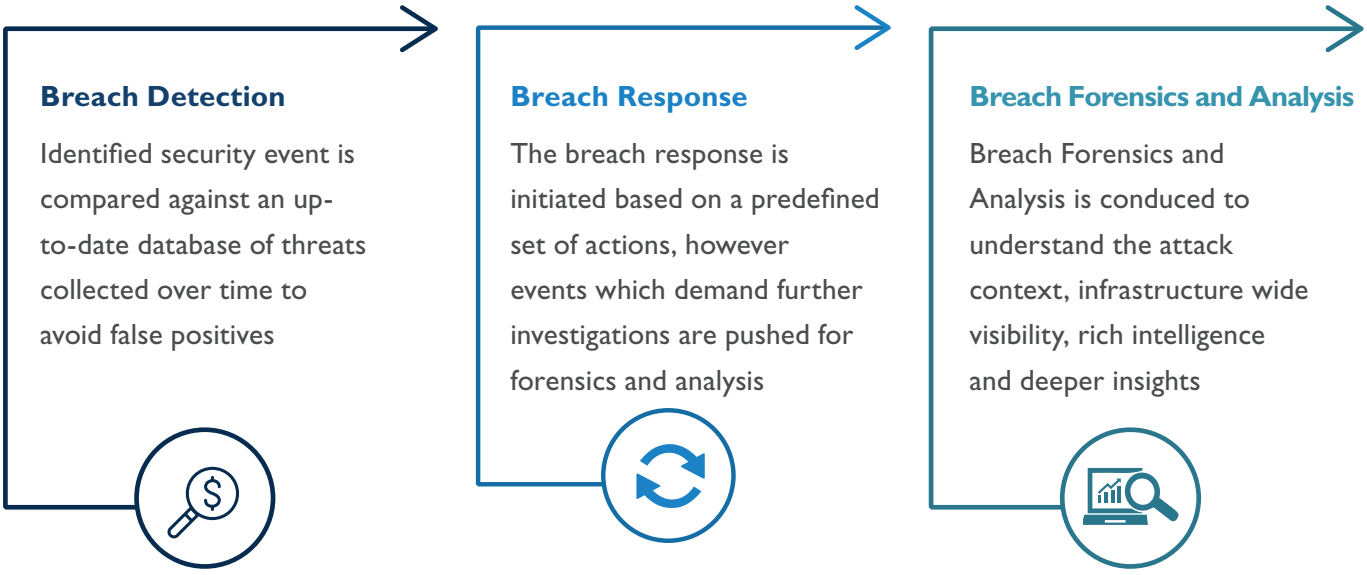
Average Economic Impact of a cyber-attack in India goes to over $ 100K

The Golden Triangle - People, Process and Technology

While the global mega trends in security are evidence of the fact how enterprises have started to re-look into re-strategizing their security narrative, CISOs are putting efforts to re-define fundamentals. Today, the dialogue is centered on People, Process and Technology, which are the key pillars of security operations. People refer to threat hunters who are trained information security professionals with the capability to proactively detect, isolate and neutralize advanced threats. Security Processes allude to Risk Analysis, Risk Management, System Auditing and Sanction Policies. Technology is complemented by threat intelligence that takes part in event detection, response and event forensics and analysis.

Next generation security architecture provides more intelligence and efficiency to fight advanced threats. The architecture is provisioned to detect, prevent, respond and manage threat actors. Security Data is collected from multiple sources within the network, web, application and endpoint to make sense of the unidentified threat by running correlation analysis. Integrating security systems with internal IT processes and functions becomes important. Security teams consisting of threat hunters are trained on these advanced security capabilities only to help them differentiate and thereafter true and false alarms.

EXHIBIT 3: A MODERN THREAT INTELLIGENCE ENGINE

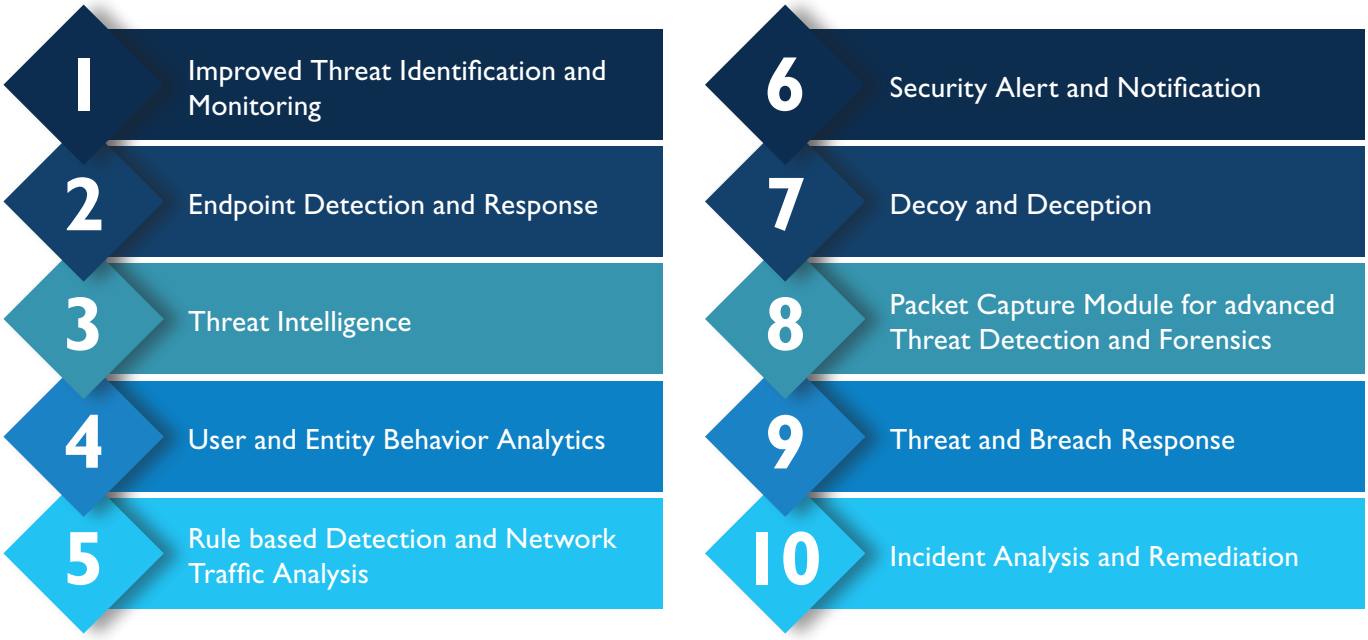


Source: Frost & Sullivan

The Next Generation Security Tools and Techniques

Advanced security tools and techniques are built around the digital assets of network, user, email, web, remote access and endpoint. They are meant for protecting not only legacy IT systems but also IoT devices and Cloud infrastructure that has become an important component of every enterprise. Next gen technologies refer to proactive threat identification before a cyber-attack. Below is the list of security processes meant for today's threat ecosystem:

EXHIBIT 4: TOP 10 NEXT GENERATION SECURITY TECHNOLOGIES AND TECHNIQUES



Source: Frost & Sullivan

So, how can enterprises leverage these advanced security technologies? Should they build in-house expertise, which is cost intensive? Or should they consider an outsourced model?

Managed Security Services is an ideal choice for managing today's security requirements.

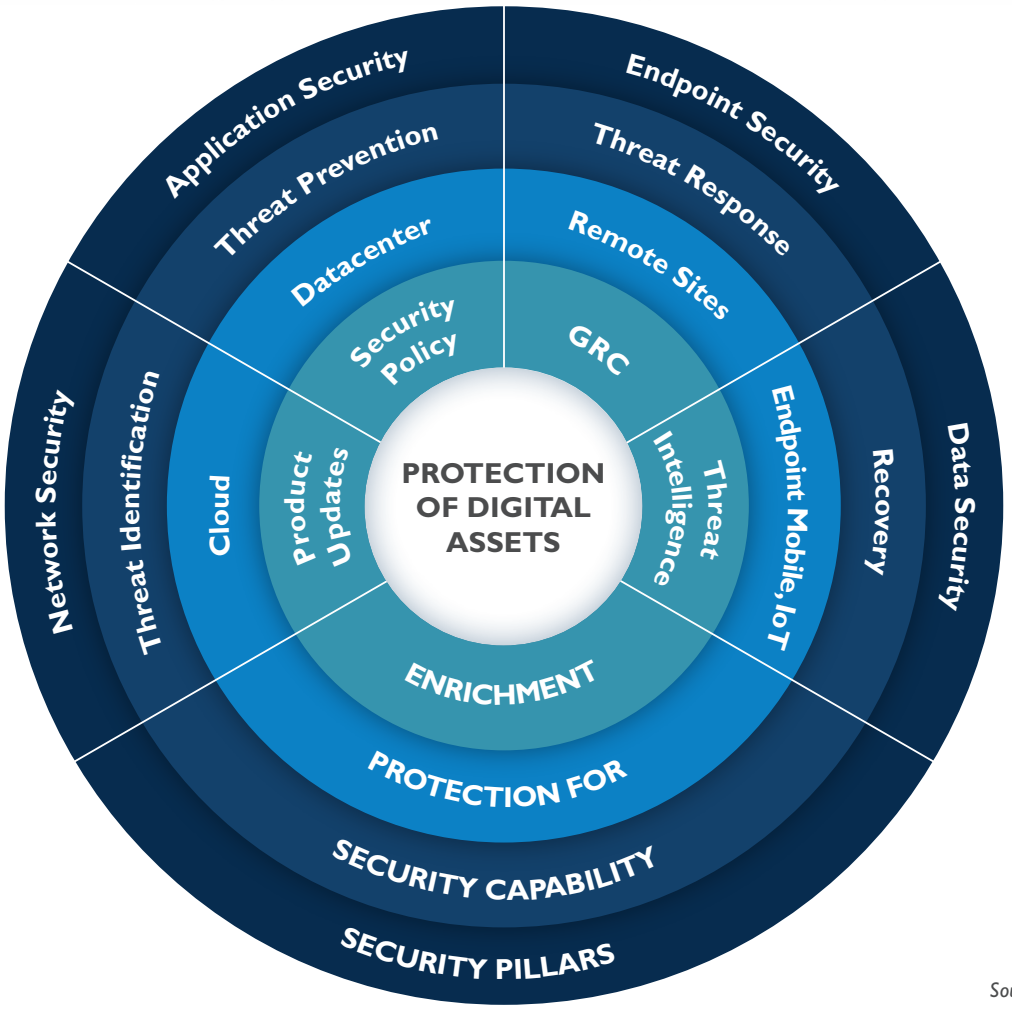
WHY ADOPT **MANAGED SECURITY SERVICES?**

Conceptually, Managed Security Services (MSS) came into existence because of enterprises' struggle to manage security issues on their own. There were too many security products, tools and software to administer and every vendor had a separate Service Level Agreement (SLA) to follow. Moreover, enterprises were not looking to invest and own costly security products as technologies are fast changing and old devices are incapable of fighting newer security threats. Traditional security products could not be scaled up or down depending on the need of the organization and hence posed challenge difficulty. As a result enterprises started looking for options that offered consumption based model (pay-as-you-use) and did not call for huge investments. The concept of MSS offered scalability through cloud managed security services, brought in easy manageability of complex security solutions, offered flexibility to the customer, provided a consumption-based billing model and helped enterprises give enterprises comprehensive suite of advanced security solutions.

> *For enterprises using a large number of security solutions, more than 50% of them agreed that it took more than a day for them to recover from a security breach*

The Building Blocks of a Modern MSS Model

EXHIBIT 5: PRIMARY ELEMENTS OF AN ADVANCED SECURITY ARCHITECTURE



Source: Frost & Sullivan

A modern Security Operations Center (SOC), which remains at the heart of the MSS model, consists of a security architecture that is designed based on today's security needs. The four key security pillars of network, application, endpoint and data support the entire structure by providing granular level security to the entire IT system. These elements are empowered to identify advanced threats (both known and unknown), prevent breaches, provide response and recover data and systems. In this digital world, where data not only resides within the corporate network, but is spread across the cloud, datacenter, remote sites and endpoints; securing each of these data hubs become highly important. A MSS provider takes responsibility of data stored in each of these data buckets by using latest security tools, a threat intelligence engine, proven policies and 24x7 monitoring by threat hunters.

The Role of a Managed Security Service Provider (MSSP)

Enterprises often spend too much time and effort in firefighting with false positives. With enterprises already crippled with limited number of security professionals, maintaining an in-house team of security resources makes little sense. The most vulnerable security threats go unnoticed and enterprises as a whole face challenges in running cyber operations from a threat assessment, containment and breach remediation perspective.

Advanced MSSPs solve the problem tactically with a fresh approach. MSSPs use Security Orchestration, Automation and Response (SOAR) solutions to collect security threats and alerts from multiple sources. Incident Response and Triage are performed using Artificial Intelligence and Human expertise to help define, prioritize and drive incident response activities as per standard workflows. These improved security solutions augment security tasks and create smart insights by running correlation analysis on collected logs and turning them into contextual alerts.

What initially took a few weeks and months is now reduced to minutes. The best in class MSSPs integrate all key elements of advanced security posture like people, methodology and technology to offer the best defense combination.

Managed Security Services are being offered by trained threat hunters who are specialized in specific areas of security and provide 360 degree coverage for enterprise protection. Continuous monitoring, detection, threat intelligence, event correlation, incident response, threat mitigation and forensics are a few of the most common managed security services offered by providers.

QUICK FACTS

- *~90% of the security events can be avoided by following the fundamentals of cyber security hygiene*
- *75% CIOs have developed IT and Security Governance for managing Cloud resources*
- *Close to 50% of them are concerned about Data Residency and Encryption of Data in Cloud*
- *More than 20% of Indian Enterprises have already enabled AI driven security techniques to improve overall threat detection capability within their technology landscape*

Source: Frost & Sullivan

Choosing the Right MSSP

With several players in the Managed Security Service space, choosing one is a tough decision. Enterprises seek providers who would be long term partners in their digital transformation journey and can be consultants in their fight against cyber-crime. Listed below are the top 6 Parameters to be considered while choosing the Right MSSP:

Exhibit 6: Points to consider while choosing the Service Provider

Local presence of a Security Operations Center (SOC)	*Enterprises should prefer MSSPs who have a local SOC in the country that helps them get access to Security Analysts easily. Also, having a SOC in the country assists enterprises in complying with industry mandates where the data or log should be stored in the country.*
Services delivered both from a Security Platform and at customer's place	*In several cases enterprises have an existing SOC within their premises and would not like to outsource the entire activity to a managed provider. Enterprises should partner MSSPs who offer both the models of CPE based services and Hosted models.*
Scalability and Flexibility of Services, Customer Friendly SLA, Multiple Delivery Models	*While enterprises move ahead in the Digital Transformation journey, they need security solutions that are scalable and fit into the maturity curve. MSSPs should adhere to SLAs that benefit the enterprise as a whole and offer tangible value proposition. Enterprises should select providers who allow customers to customize their requirements.*
Team of Threat Hunters and Domain Experts	*The SOC team should be a diverse set of threat hunters that includes analysts, investigators, incident handlers, forensic experts, data scientists, SOC architects and product specialists.*
Billing based on a consumption based model that provides the best cost proposition	*With the managed model, enterprises should be able to extract the benefits of pay-as-use model that is cost effective and offers low TCO.*
Has Depth and Width of MSS offerings with access to Advanced Technologies	*Enterprises should consider service providers that have purpose built technology for MSS with threat detection, security intelligence and advanced analytics to detect sophisticated attacks. Need to validate how this technology examines logs, detect threats and handles false positives.*

Source: Frost & Sullivan

Expectations from a MSSP

Once an agreement has been signed, the enterprise should expect the MSSP to deliver on expectations as set in the SLA. Enterprises and MSSP together should design the agreement in accordance with strategy, people, process, technology, environment and improvement; that remains missing in most cases. A world-class provider takes care of these individual buckets from a security perspective to improve the comprehensive security posture.

PROCESS

The Service Provider is expected to be a security advisor to CIOs/CISOs in building well-defined internal processes that provide consistent/ reliable operations and repeatable outcomes.

TECHNOLOGY

MSSPs should work closely with the enterprise to develop a multi-year technology roadmap that would improve SOC capabilities over time.

Exhibit 7: Expectations from a Managed Security Provider

STRATEGY

MSSPs should ensure that they build an integrated security framework that provides measurable impact on overall enterprise IT.

CONSTANT IMPROVEMENT

While MSSPs design the multi-year roadmap for their SOC, it is expected that they take into consideration the process of continuous improvement in their SOC capabilities to fight the modern day threat landscape.

PEOPLE

MSSPs should leverage in-depth knowledge about security products/ tools and provide skilled resources as enterprises build SOC capabilities from scratch. Managed providers can be treated as long-term partners in the overall security journey.

Source: Frost & Sullivan

NTT-NETMAGIC
MANAGED SECURITY SERVICES

Approach to Comprehensive Security

Over the years, working with a large base of Indian customers, NTT-Netmagic Managed Security Services has earned substantial reputation and customer confidence in the domestic market. The service provider's MSS offerings help enterprises minimize security risks, protect critical information and reduce operating cost. NTT-Netmagic has 20+ security service lines with SOCs present in Mumbai and Chennai.

In the effort to fight security breaches, NTT-Netmagic takes a comprehensive approach to counter threat vectors. It has a model that takes into account all the four pillars of the security architecture – network, application, endpoint and data – and offers 360 degree security coverage. The model is built to address next generation threats that traditional security products fail to provide and secures assets, users and data from lone rangers, hacktivists, cyber-crime syndicates and nation sponsored cyber criminals.

NTT-Netmagic SOCs are equipped with advanced cyber mechanisms and techniques. This includes:

- Automation, Orchestration & Response
- Threat Intelligence to move from Passive to Active Defense
- Threat Hunting and Breach Response
- Pre-defined Metrics for measurement of effectiveness
- Identifying known unknowns and unknown unknowns

EXHIBIT 8: ADVANCED CAPABILITY OF NTT-NETMAGIC SOC

PREVENTION & DETECTION

- IPS
- IDAM/PIM
- Cloud Security
- End Point Detection
- Email Security

REPORTING AND IMPROVEMENT

- Use Case
- Development
- Threat Modelling
- Maturity Assessment
- Training

INCIDENT RESPONSE & TICKETING

- Threat Hunting
- EDR
- Red Team
- Forensics
- User Behavior
- Machine Data Analytics

ORCHESTRATION, AUTOMATION & ANALYSIS

Analytics & Machine Learning

Orchestration Platform

Threat Intelligence

Source: NTT-Netmagic

NTT-Netmagic Security Services are meant for enterprises that have embraced some form of digitalization irrespective of the stage in the maturity curve. Most services offered by the provider can be scaled up or down as and when needed to match the DT requirements of enterprises. NTT-Netmagic's Pay-as-You use model helps customers plan internal cost most effectively and plug unwanted cost outflow.

EXHIBIT 9: NTT-NETMAGIC'S COMPREHENSIVE SECURITY MODEL

Service Type

- NTT-Netmagic's Platform Services
- Customer On-premise Solutions

Model

- Offered as an OPEX
- Offered as CAPEX and OPEX

SOC Type

- NTT-Netmagic shared SOC
- On-premise, Remote, Hybrid SOC

Network Security

- DDoS Protection
- Managed IDS & IPS
- Network VA and PT
- Server Host Protection

Application Security

- Application VA and PT
- Web Application Firewall
- Exposure Monitoring
- Anti-phishing and Malware Protection

SIEM/SECURITY ANALYTICS DECOY AND DECEPTION AUDITS AND ASSESSMENT VULNERABILITY PATCH MANAGEMENT

Endpoint Security

- Secure Web Gateway
- Email Gateway
- Antivirus & Anti-malware
- Anti APT Protection

Data Security

- Host DLP
- Network DLP
- Database Activity Monitoring
- Privileged ID Management

Deliverables

- Standardized Deliverables
- Customized Deliverables

Billing

- Pay as you grow
- Customized TCO

Source: NTT-Netmagic, Frost & Sullivan

NTT-Netmagic Advantage

Being a prominent managed service provider, NTT-Netmagic brings to the table the best of both worlds – technology and people. It has built a security portfolio that is meant for advanced threat actors and leverages next generation technologies. Mentioned below are the success factors and primary differentiators for the company:

- Comprehensive security portfolio from network to endpoint and application to data
- Advanced SOC capabilities: Prevention & Detection, Incident Response, Security Orchestration and Reporting, Threat Intelligence
- A framework for quantifying the cybersecurity risk to the board
- The option to choose between on-premise solutions and platform based offerings
- Commercial modeling available as CAPEX or OPEX
- MDR (Manage, Detect and Respond) services with choice of onsite, offsite and hybrid teams

THE WAY AHEAD IN MANAGED SECURITY SERVICES

The Managed Security Services market remains the fastest growing segment within the all-inclusive security stack. Demand from enterprises is expected to continue as MSSPS come up with flexible security plans, SOC models (on-premise, remote, shared and hybrid), deliverable types and multiple payment options. Providers would lower the TCO for customers and agree to customer friendly SLAs. The expertise of an MSSP would be judged purely on its capability to leverage emerging security concepts like threat hunting, security automation, red teaming, forensics, UEBA and investigation. Providers that complement these security technologies with people and process would be the trusted partners.

> *Moving ahead, enterprises would initiate a conversation that focuses on 5 strong pillars of threat identification, prevention, response, remediation, and advanced security posture*

About NTT Ltd.

NTT Ltd. is a leading global technology services company bringing together 28 brands including NTT Communications, Dimension Data, and NTT Security. We partner with organizations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital, and secure. As a global ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace that spans 57 countries and regions, trades in 73 countries and regions, and delivers services in over 200 countries and regions. Together we enable the connected future. Visit us at our new website https://hello.global.ntt

About NTT-Netmagic

NTT-Netmagic, a wholly-owned subsidiary of NTT, is India's leading Managed Hosting and Multi-Cloud Hybrid IT solution provider serving more than 2000 enterprises globally. Headquartered in Mumbai, NTT-Netmagic also delivers Remote Infrastructure Management (RIM) services to various enterprise customers globally across Americas, Europe and Asia-Pacific region. The Company was the first in India to launch services – Cloud Computing, Managed Security, Disaster Recovery-as-a-Service (DRaaS) and Software-Defined Storage. NTT-Netmagic has been recognized with 4 awards at the CIO Choice 2019, 2 awards at the Datacenter Dynamics India 2019, and Frost & Sullivan India ICT Awards 2018. To learn more, visit us at: www.netmagicsolutions.com

About Frost & Sullivan

For over five decades, Frost & Sullivan has become world-renowned for its role in helping investors, corporate leaders and governments navigate economic changes and identify disruptive technologies, Mega Trends, new business models and companies to action, resulting in a continuous flow of growth opportunities to drive future success. Contact us: Start the discussion

www.frost.com