360 Quadrants

MANAGED SECURITY SERVICES (MSS)

COMPANY EVALUATION REPORT, 2025

(Market Dynamics, Competitive Landscape, and Key Players)

PUBLISHED BY:
MARKETSANDMARKETS

INFORMATION &
COMMUNICATIONS TECHNOLOGY

360Quadrants, a specialized division of MarketsandMarkets™, delivers comprehensive quadrant analyses for a wide array of emerging technologies and markets, including start-ups. Our evaluation methodology hinges on two critical parameters: market presence and product footprint. This approach facilitates a graphical representation of competitive positioning across four key categories: leaders, contenders, innovators, and emerging companies. In addition, we meticulously classify start-ups into progressive companies, responsive companies, dynamic companies, and starting blocks. Our expertise equips organizations with insights on market leaders across over 6000 micro markets, enabling a detailed comparison of vendor capabilities and performance. At 360Quadrants, we ensure that each quadrant adheres to the highest standards, empowering our clients to navigate complex market dynamics with precision and confidence.

Copyright © 2025 360Quadrants
All Rights Reserved. This document contains highly confidential information and is the sole property of 360Quadrants. No part of it shall be circulated, copied, quoted, or otherwise reproduced without the prior written approval of 360Quadrants.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 MARKET DEFINITION

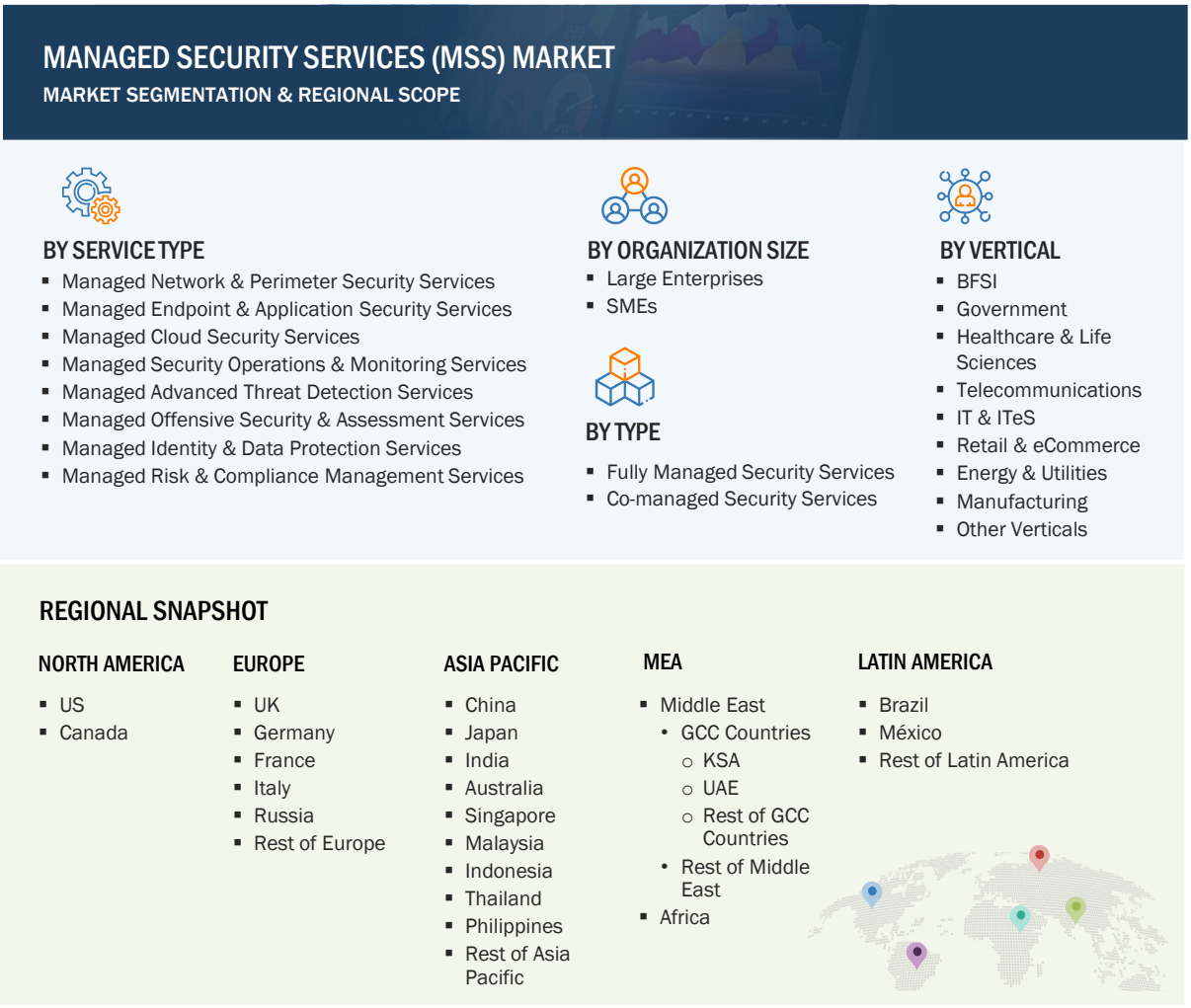
Considering the sources and associations or Forum's views on managed security services, MarketsandMarkets defines it as follows:

"Managed security services are the management of an organization's security infrastructure from an outside or third-party location. Outsourced security services, third-party security services, and as-a-service are the terms associated with managed security services."

1.2 STUDY SCOPE

The study analyzes the global managed security services market since 2019, based on contemporary market trends and developments, and its potential growth from 2025 to 2030. It provides detailed market trends, vendors' market shares, market size, forecasts, and analysis of the key players in the market.

1.2.1 MARKET SEGMENTATION AND REGIONAL SCOPE



Note: Other verticals include education, travel and hospitality, and media & entertainment.

The Rest of Europe includes Ireland, Spain, the Netherlands, Switzerland, Poland, and the Czech Republic, among others.

The Rest of the Asia Pacific includes Vietnam and South Korea, among others.

The Rest of GCC Countries include Bahrain, Kuwait, Oman, and Qatar.

The Rest of Middle East includes Israel, Egypt, Turkey, Iraq, Iran, Jordan, Lebanon, and Syria, among others.

The Rest of Latin America includes Peru, Argentina, Colombia, and Chile, among others.

Source: Industry Experts and MarketsandMarkets Analysis

1.2.2 INCLUSIONS AND EXCLUSIONS

CATEGORY	INCLUSION	EXCLUSION
Service Type	▪ Comprehensive coverage of managed services across network & perimeter, endpoint & application, cloud, security operations & monitoring, advanced threat detection, offensive security, identity & data protection, and risk & compliance ▪ Services delivered via outsourced, co-managed, or fully managed models, including 24/7 SOC, MDR/XDR, SIEM-as-a-service, managed IAM, managed DLP, managed vulnerability management, and managed compliance monitoring ▪ SOC as a Service, MDR/XDR covered as integral parts of MSS delivery (not standalone markets). An overall analysis of manual and automated managed security services ▪ Security types provided by vendors specific to managed security services	▪ Hardware & infrastructure (routers, switches, servers, appliances, BYOD devices, etc.) not directly tied to MSS delivery ▪ Particular technical aspects of security types ▪ Open-source managed security services ▪ Overlaps/double counting among managed security types of services ▪ No separate market sizing for SOC or XDR (included under broader categories (Security Ops & Monitoring, MDR)) ▪ Services offered in the subscription packages ▪ Consulting/advisory-only projects (audits, one-time pen tests, strategy roadmaps, etc.), not part of ongoing MSS engagements
Type	▪ Separate analyses of fully managed and co-managed security services	▪ Multi-platform security management
Organization Size	▪ SMEs with an employee strength ranging between 1 and 1,000 ▪ Large enterprises with an employee strength of more than 1,000	▪ Local or unlisted organizations ▪ Recent start-ups founded in the past six months
Vertical	▪ B2B market analysis ▪ Global analysis of key verticals, such as BFSI, government, healthcare & life sciences, telecommunication, IT & ITeS, retail & eCommerce, energy & utilities, manufacturing, and others ▪ Other verticals, including education, travel and hospitality, and media & entertainment	▪ B2C market analysis ▪ Cross-segmentation study and analysis ▪ In-depth analysis of each vertical related to a particular country or region ▪ A separate analysis of other verticals, such as education, travel and hospitality, and media & entertainment

Region	▪ North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America ▪ US, Canada, UK, Germany, France, Italy, Russia, China, Japan, India, Australia, Singapore, Malaysia, Indonesia, Thailand, Philippines, Brazil, and Mexico ▪ Other regions, such as the rest of Europe, the rest of Asia Pacific, the rest of the Middle East & Africa, and the rest of Latin America, limited to the countries included in the scope.	▪ A separate analysis of countries in the rest of Europe, the Asia Pacific, the Middle East & Africa, and Latin America ▪ Analysis of local markets

Source: MarketsandMarkets Analysis

1.3 STAKEHOLDERS

- Chief Technology and Data Officers
- Consulting Service Providers
- Managed Security Service Professionals
- Business Analysts
- Information Technology (IT) Professionals
- Government Agencies
- Investors and Venture Capitalists
- Small and Medium-sized Enterprises (SMEs) and Large Enterprises
- Third-party Providers
- Consultants/Consultancies/Advisory Firms
- Managed and Professional Service Providers

2 EXECUTIVE SUMMARY

Cyber threats continue to evolve in speed, complexity, and impact—encompassing ransomware, advanced persistent threats (APTs), phishing, and zero-day exploits. Organizations are under relentless pressure to protect assets, ensure regulatory compliance, and maintain operational resilience. Managed security services (MSS), which encompass outsourced threat monitoring, detection, response, and compliance, have become a strategic imperative for businesses across sectors.

MSS has emerged as a cornerstone of modern cybersecurity strategy, enabling organizations to safeguard networks, endpoints, applications, cloud workloads, and critical data against increasingly sophisticated threats. With the rise of digital transformation, remote work adoption, cloud migration, and IoT proliferation, enterprises face a rapidly expanding attack surface that is difficult to secure with internal resources alone. MSS providers (MSSPs) deliver continuous threat monitoring, detection, and response, leveraging global threat intelligence, advanced analytics, and security operations expertise to mitigate risks while ensuring regulatory compliance.

KEY COMPONENTS OF MSS INCLUDE:

- Network & Perimeter Security Services: Encompasses managed firewalls, IDS/IPS, VPNs, and DDoS protection. These services establish the first line of defense, ensuring secure connectivity and safeguarding enterprise perimeters.
- Endpoint & Application Security Services: Protects devices and applications through managed EDR, anti-malware, patching, and application whitelisting. With hybrid work and BYOD environments, these services help organizations reduce endpoint vulnerabilities.
- Cloud Security Services: Focuses on securing cloud workloads and SaaS applications with CSPM, CWPP, CASB, SSPM, and container security management. As cloud adoption accelerates, these solutions provide visibility, compliance enforcement, and workload protection.
- Security Operations & Monitoring Services: Includes SOC-as-a-service, managed SIEM, incident response, and OT/ICS SOC monitoring. These offerings ensure 24/7 monitoring, rapid incident containment, and operational resilience.
- Advanced Threat Detection Services: MDR, MXDR, threat intelligence, threat hunting, ransomware recovery, and disaster recovery-as-a-service. This segment addresses sophisticated threats that evade traditional defenses, enabling proactive response.
- Offensive Security & Assessment Services: Managed penetration testing, vulnerability management, red teaming, ICS/SCADA testing, and source code analysis. These services simulate adversary behavior to uncover weaknesses before attackers exploit them.
- Identity & Data Protection Services: Managed IAM, MFA, SSO, DLP, encryption, and identity federation. With identity-based attacks on the rise, MSSPs deliver centralized control and compliance-ready data protection.
- Risk & Compliance Management Services: Includes compliance reporting, GRC integration, phishing simulation, insider threat monitoring, and security training-as-a-service. These services ensure regulatory adherence and foster a culture of cyber resilience.

TRENDS IN THE MSS MARKET:

- Expanding Digital Footprint & Evolving Threats: Rapid cloud adoption, remote work, and IoT proliferation have dissolved traditional perimeters, increasing enterprise exposure. This expanding attack surface, along with more sophisticated adversarial tactics, is driving the need for continuous monitoring, advanced detection (MDR/MXDR), and SOC-as-a-service capabilities.
- Regulatory Complexity & Compliance Pressure: Heightened enforcement of GDPR, HIPAA, PCI-DSS, DORA, and NIS2 mandates organizations to strengthen cybersecurity controls. MSS solutions provide audit-ready compliance, automated reporting, and risk frameworks, which are particularly vital in heavily regulated sectors such as BFSI, healthcare, and government.
- Cybersecurity Skills Gap & Cost Efficiency: The global shortage of cybersecurity professionals and high costs of in-house SOCs and tools are steering enterprises toward MSSPs. These providers offer on-demand access to scalable expertise, enabling real-time monitoring and response without significant capital expenditure.
- Technological Differentiation via AI & Automation: MSSPs are embedding AI/ML, SOAR, and threat intelligence integration into their offerings, improving detection accuracy, automating response workflows, and reducing dwell times. MXDR and zero-trust aligned services are increasingly becoming key differentiators.
- Growth in Regional Markets & Demand from SMEs: Emerging markets, particularly in Asia Pacific and the Middle East & Africa, are witnessing accelerated MSS adoption due to smart city initiatives, critical infrastructure investments, and digitalization efforts. Concurrently, SMEs, with tighter budgets but growing cybersecurity exposure, are adopting MSS for scalable and affordable protection.

The MSS market is witnessing strong growth as enterprises and governments recognize the need for cost-effective, outsourced security operations. The global MSS market is projected to grow from USD 39.47 billion in 2025 to USD 66.83 billion by 2030, at a CAGR of 11.1%. This demand is driven by the shortage of skilled cybersecurity professionals, rising regulatory pressures (GDPR, HIPAA, PCI-DSS, DORA, NIS2), and the increasing cost of cybercrime.

TABLE 1 MANAGED SECURITY SERVICES MARKET SIZE AND GROWTH, 2019–2024 (USD MILLION)

Particular	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Market Size	18,468.6	21,624.9	24,807.1	28,060.4	31,498.9	35,270.4	13.8%
Y-o-Y	-	17.1%	14.7%	13.1%	12.3%	12.0%	-

Source: MarketsandMarkets Analysis

TABLE 2 MANAGED SECURITY SERVICES MARKET SIZE AND GROWTH, 2025–2030 (USD MILLION)

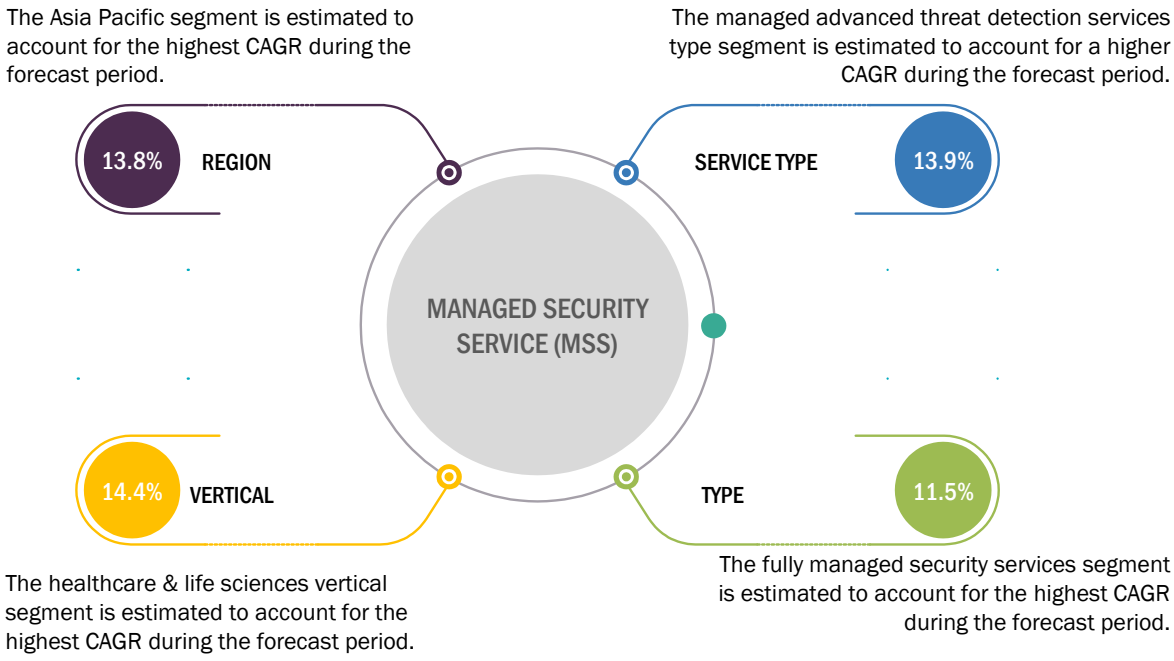
Particulars	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Market Size	39,472.3	44,048.9	48,989.6	54,492.5	60,381.0	66,832.8	11.1%
Y-o-Y	11.9%	11.6%	11.2%	11.2%	10.8%	10.7%	-

Note: Y-O-Y for 2025 is calculated based on the values calculated for 2024.

Source: MarketsandMarkets Analysis

The MSS market is studied across five regions, namely North America, Europe, Asia Pacific, Latin America, and the Middle East & Africa. IBM (US), NTT (Japan), LevelBlue (US), Accenture (Ireland), DXC Technology (US), Secnap (US), DigitalXRAID (UK), Deloitte (US), Secureworks (US), Trustwave (US), Verizon (US), Fujitsu (Japan), HPE (US), TCS (India), Atos (France), Orange Cyberdefense (France), Rapid7 (US), TrendMicro (Japan), Kudelski Security (Switzerland), CrowdStrike (US), F5 (US), Capgemini (France), Infosys (India), Lumen (US), Kroll (US), Netsurion (US), Atlas Systems (US), Cipher (US), RSI Security (US), SecurityHQ (UK), Lightedge (US), LRQA (UK), Teceze (UK), CyFlare (US), Ascend Technologies (US), Avertium (US), and TrustNet (US) are the key players profiled in the report.

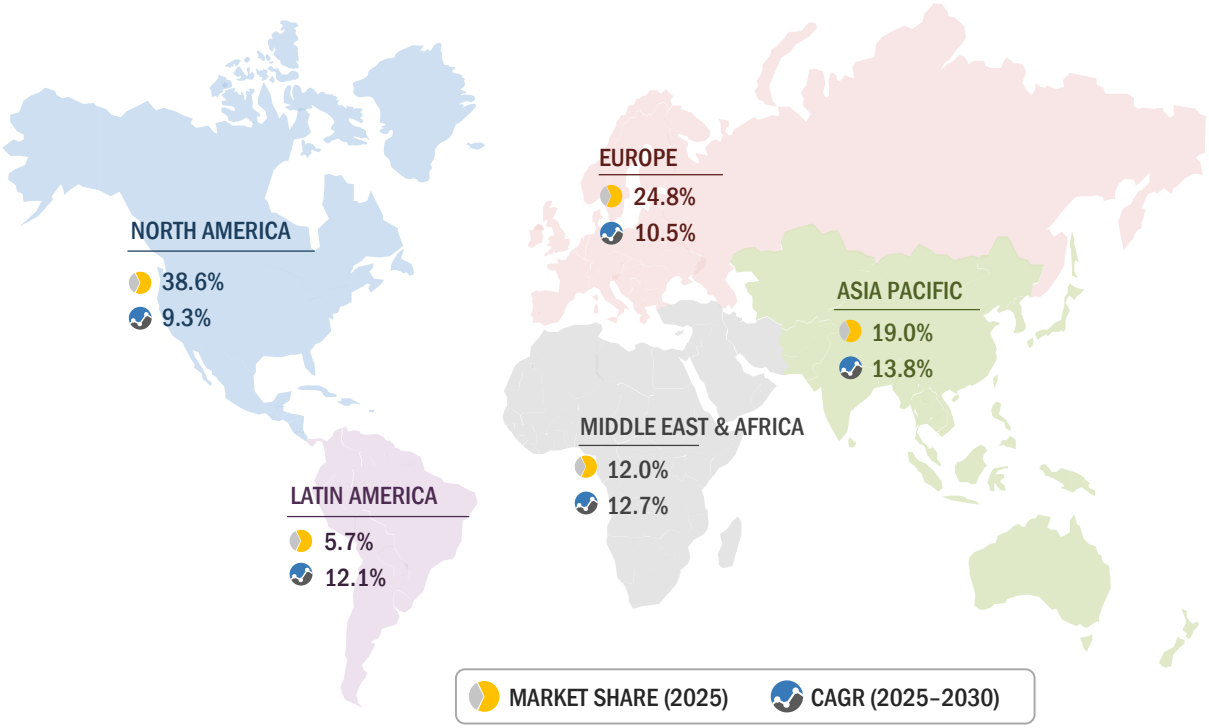
FIGURE 1 MANAGED SECURITY SERVICES MARKET: SEGMENTAL SNAPSHOT



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

The chart highlights the segments expected to witness the highest growth in the MSS market during the forecast period. By service type, the managed advanced threat detection services segment is projected to grow at the highest CAGR, driven by rising demand for proactive detection, response, and recovery against advanced cyber-attacks. By type, the fully managed services segment is set to expand rapidly as enterprises increasingly outsource end-to-end security operations to MSSPs. On the vertical side, the healthcare & life sciences segment is expected to record the strongest growth, owing to stringent compliance requirements and the need to protect sensitive patient data. Regionally, the Asia Pacific is projected to grow at the fastest pace, supported by digital transformation initiatives, regulatory mandates, and increasing adoption of cloud-based security models.

FIGURE 2 MANAGED SECURITY SERVICES MARKET: REGIONAL SNAPSHOT



Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

North America is projected to be the leading region in terms of adopting and developing managed security services. Asia Pacific is projected to record the highest CAGR. This market growth is attributed to various factors, including the increasing need to adhere to stringent regulations, the growing presence of MSS vendors, increasing government support, growing awareness of managed services utilities, and rising return on investments. The public and private sectors invest heavily to increase organizations' operational efficiency and productivity, propelling the demand for managed security services. The increasing security concerns, regulations, and compliance contribute to the adoption of MSS in Asia Pacific.

3 MARKET OVERVIEW AND INDUSTRY TRENDS

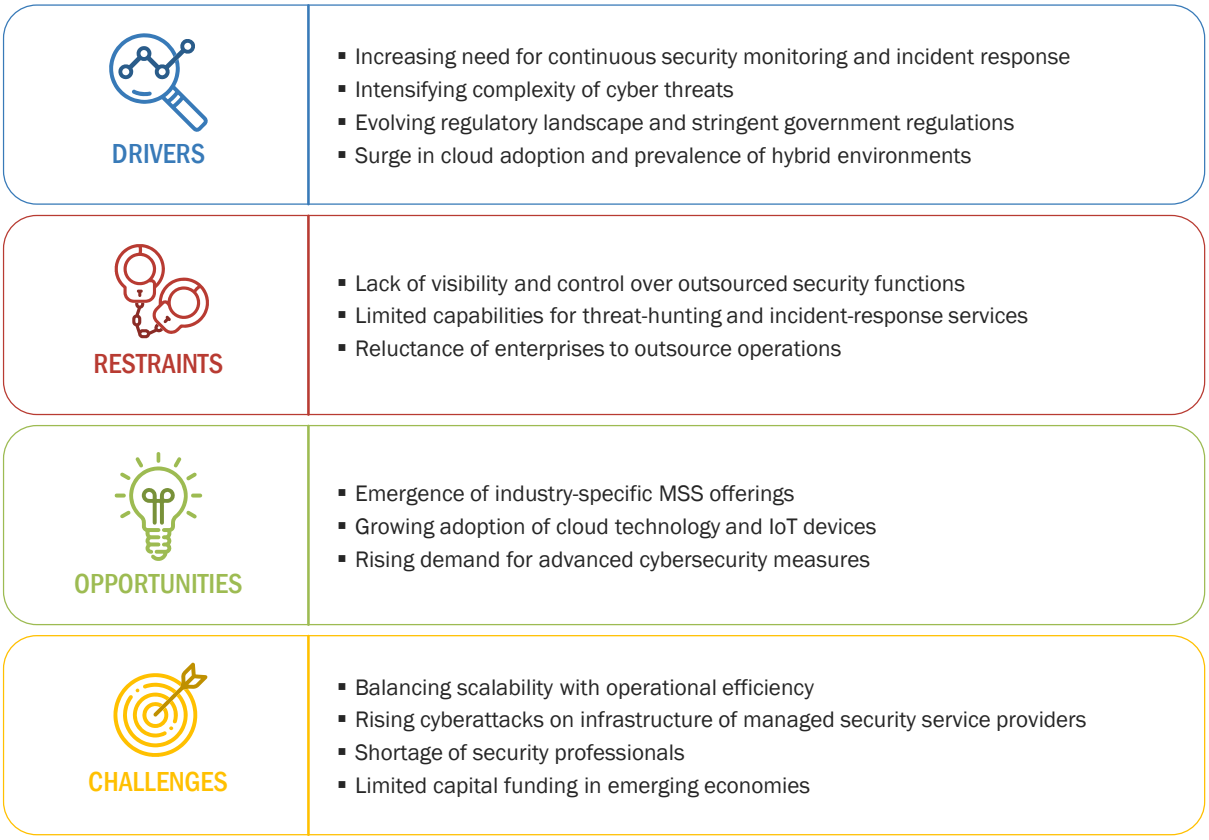
3.1 INTRODUCTION

The market overview chapter offers detailed information about the factors responsible for the growth of the managed security services (MSS) market. It comprises market dynamics, such as drivers, restraints, opportunities, and challenges. The market is expected to grow significantly with the increasing adoption of MSS in the BFSI, government, retail, manufacturing, and other verticals. The consistent rise in the demand for the security of IT resources is expected to drive the market. With a new approach to cloud-based software & services, organizations are deploying cloud-based management software due to its cost-effective, flexible, and agile nature. Cloud-based software and services assist organizations in growing within the economy. The key market players include IBM, Accenture, Infosys, NTT, SecureWorks, and DXC Technology.

3.2 MARKET DYNAMICS

The MSS market is expected to be lucrative for technology vendors and projected to witness substantial growth in the next five years due to stringent government regulations; a surge in Bring Your Own Device (BYOD), Choose Your Own Device (CYOD), and Work From Home (WFH); and rising security breaches and sophisticated cyberattacks across enterprises. These factors are expected to propel governments and private firms to deploy or develop managed security solutions in the coming years.

FIGURE 3 MANAGED SECURITY SERVICES MARKET: MARKET DYNAMICS



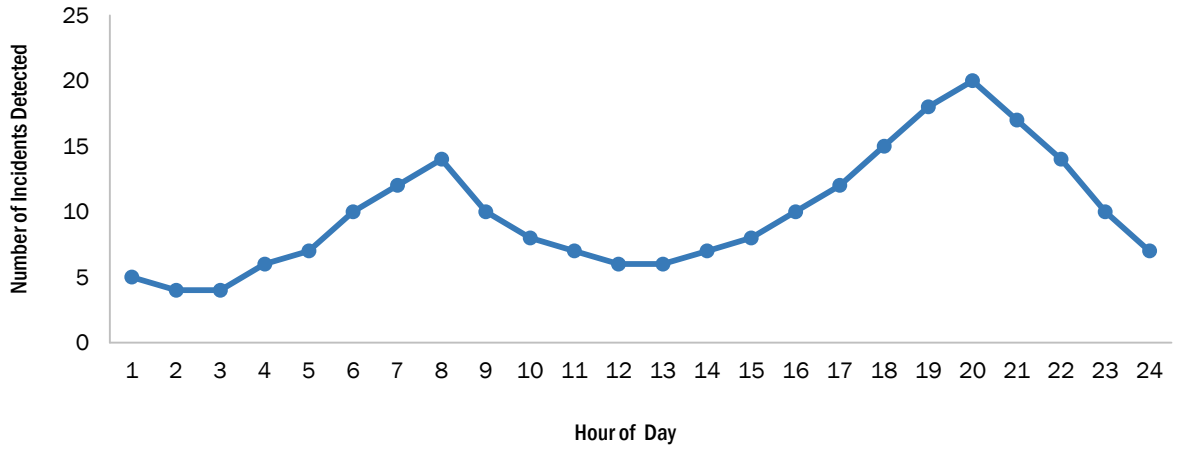
Source: Secondary Research, Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

3.2.1 DRIVERS

3.2.1.1 Increasing need for continuous security monitoring and incident response

The increasing need for 24/7 security monitoring and incident response is crucial in the MSS market, as organizations face a relentless wave of cyber threats that do not adhere to business hours. Modern cyberattacks ranging from advanced persistent threats (APTs) to zero-day exploits can occur at any time, often targeting off-hours to exploit reduced staffing and slower response times. The chart below depicts that cyber incidents often peak during late-night and early-morning hours, emphasizing the critical need for continuous monitoring.

FIGURE 4 DETECTED SECURITY INCIDENTS OVER A 24-HOUR PERIOD



Source: checkpoint.com, darktrace.com, paloaltonetworks.com, and MarketsandMarkets Analysis

This timing trend reinforces why traditional 9–5 security operations are no longer sufficient; modern MSS must operate across all time zones and non-business hours to be truly effective.

According to IBM's 2024 Cost of a Data Breach Report, breaches identified and contained within 200 days cost USD 1.26 million less than those that take longer, underscoring the importance of continuous monitoring. Many businesses, particularly small to mid-sized enterprises, lack the internal resources or expertise to maintain round-the-clock vigilance. This creates a strong demand for MSS providers who offer round-the-clock security operations centers (SOCs), real-time threat detection, and rapid incident response capabilities.

3.2.1.2 Intensifying complexity of cyber threats

The increasing complexity of cyber threats is a key catalyst driving the growth of the MSS market. In recent years, the cybersecurity landscape has witnessed a surge in sophisticated and multifaceted threats that demand advanced defense mechanisms. Cybercriminals are deploying highly intricate tactics, such as advanced persistent threats (APTs), zero-day exploits, and polymorphic malware, making it challenging for organizations to defend their digital assets adequately.

Advanced Persistent Threats (APTs) are known for their stealthiness and can be challenging to detect. They require ongoing monitoring and sophisticated threat intelligence for effective mitigation. Zero-day exploits, which target vulnerabilities in software that are not yet known to vendors, present a significant obstacle to traditional security measures. This situation underscores the necessity for rapid response capabilities. Polymorphic malware variants are designed to evade signature-based detection, requiring dynamic and adaptive security solutions. This complexity extends to multi-vector attacks, insider threats, supply chain vulnerabilities, and cloud security challenges, making the cybersecurity landscape more intricate and challenging than ever before.

In response to this evolving threat landscape, organizations are recognizing the limitations of relying solely on in-house security measures. The shortage of skilled cybersecurity professionals exacerbates this challenge, prompting businesses to turn to MSS providers. These providers offer a comprehensive suite of services, including advanced threat detection, real-time monitoring, incident response, and expertise in handling diverse and complex cyber threats. MSS providers leverage cutting-edge technologies, such as artificial intelligence and machine learning, to analyze patterns, detect anomalies, and respond swiftly to emerging threats.

3.2.1.3 Evolving regulatory landscape and stringent government regulations

The evolving regulatory landscape is a crucial factor in propelling the growth of the MSS market. Governments and industry regulators worldwide are enforcing strict data protection and industry-specific compliance standards in response to the increasing complexity and frequency of cyber threats. Regulations such as GDPR and CCPA mandate organizations to implement robust cybersecurity measures to safeguard sensitive data, while industry-specific regulations require tailored security solutions.

MSS providers help organizations navigate these regulatory frameworks by providing continuous monitoring, incident response planning, and specialized services aligned with global and regional compliance variations. As noncompliance can lead to severe penalties and reputational damage, businesses are turning to MSS providers to ensure ongoing adherence to regulatory requirements, effectively manage cybersecurity risks, and adopt emerging technologies in line with evolving regulatory expectations. The growth of the MSS market is directly linked to its ability to provide comprehensive solutions that address the dynamic and challenging landscape of cybersecurity regulations.

3.2.1.4 Surge in cloud adoption and prevalence of hybrid environments

As businesses increasingly embrace cloud technologies for enhanced agility and scalability, the intricate security landscape demands specialized solutions. The surge in cloud adoption and the prevalence of hybrid environments are driving the MSS market. Hybrid environments amalgamate on-premises and cloud infrastructure, introducing unique challenges that necessitate a unified approach to security. MSS providers offer tailored solutions to address cloud-specific threats, providing continuous monitoring, advanced threat detection, and incident response capabilities across diverse environments. The flexibility, scalability, and seamless integration with cloud service providers position MSS as a crucial element in safeguarding digital assets in this dynamic technological landscape. Organizations recognize the imperative of leveraging MSS to ensure comprehensive security measures that span traditional and cloud-based infrastructures, making it a pivotal market driver in the contemporary business landscape.

3.2.2 RESTRAINTS

3.2.2.1 Lack of visibility and control over outsourced security functions

Lack of visibility and control over outsourced security functions restrains the market growth, particularly for enterprises with complex or highly regulated environments. When security operations are handed off to a third-party provider, organizations often face challenges in maintaining real-time oversight of threat intelligence, incident handling, and compliance reporting. This lack of transparency can hinder internal decision-making, delay responses during active threats, and reduce overall trust in the MSS provider.

According to a 2023 Gartner survey, 47% of IT leaders cited “loss of control” as a key concern when outsourcing cybersecurity functions. This can become a deal-breaker for finance, healthcare, and government sectors where security and compliance are tightly interconnected. Additionally, the inability to customize monitoring rules or access raw telemetry data can limit the value that MSS brings to more mature security teams, further curbing adoption. Thus, the minimal visibility and control restrain the market by reducing customer trust, slowing adoption among security-mature organizations, and limiting appeal in regulated industries that require granular control and oversight.

3.2.2.2 Limited capabilities for threat-hunting and incident-response services

Many managed security service providers only provide security log monitoring services, which limits their ability to conduct detailed security incident investigations. To provide effective services, they must integrate their solutions into client processes such as change management and access management. Access to security tools such as Microsoft Cloud App Security and endpoint protection is also necessary to eliminate false positives and provide meaningful alerts to clients.

However, since MSS are built on specific security solutions, they do not integrate well with clients' existing tools. As a result, the existing tools may not have visibility into all security logs and environments, leading to several false positives and uncalled threat alerts. Inadequate interoperability and integration among these security tools can hamper the organization’s security posture.

3.2.2.3 Reluctance of enterprises to outsource operations

Enterprises opt for a third-party service provider if they lack the necessary in-house expertise or if they face budgetary constraints. However, this decision involves several critical considerations, such as the service provider’s infrastructure security, the effectiveness of the cybersecurity technology used, the availability of real-time support, and the overall decision to migrate to security-as-a-service. The service provider’s infrastructure needs to be secure and sophisticated enough to effectively counter the latest threats. Since the infrastructure may contain vital data from multiple organizations, it is highly vulnerable to repeated and complex attacks. This can discourage companies from entrusting their data to such service providers.

In certain situations, the higher management of organizations might be hesitant to give up control over critical aspects of their infrastructure. Companies may have reservations about letting managed security service providers oversee their entire system architecture in case of a security breach. Other factors, such as hidden fees, service quality, and lack of trust in service providers, may restrict the market growth. However, experts suggest that if these providers can consistently prove their reliability to upper-level management, businesses can benefit from improved security and profits and gain greater access to managed security service providers.

3.2.3 OPPORTUNITIES

3.2.3.1 Emergence of industry-specific MSS offerings

The emergence of industry-specific MSS offerings represents a significant opportunity in the MSS market, as organizations increasingly seek tailored solutions that address their unique regulatory, operational, and threat landscapes. The healthcare, finance, energy, and manufacturing industries face highly specialized risks and compliance demands, such as HIPAA in healthcare, PCI-DSS in finance, or NERC CIP in energy, that generic security services often fail to adequately address.

MSS providers that can deliver vertical-specific threat intelligence, policy enforcement, and compliance reporting gain a competitive edge by aligning closely with customer needs. According to Frost & Sullivan, MSS solutions designed for specific industries are expected to grow at a faster rate than generic offerings, as enterprises prioritize context-aware security that integrates seamlessly with sector-specific workflows. This trend opens new revenue streams and allows MSS vendors to establish deeper partnerships with clients, enhancing retention and trust. By investing in vertical specialization, MSS providers can position themselves as strategic security allies rather than just outsourced service providers.

3.2.3.2 Growing adoption of cloud technology and IoT devices

IoT refers to a system of interconnected computing devices and machines that can transfer data over a network without human intervention. However, with the rapid development of IoT, the security concerns for these devices have also increased. As more machines get connected to a single network, these connected devices are vulnerable to cyberattacks. For instance, in the automobile sector, companies are focusing on developing independent and self-driving cars. However, due to automation, the dependency of cars on software is set to rise, making the installed systems more susceptible to cyberattacks. IoT has become widespread, but integrating such devices with machines will increase malware attacks, which could compromise hefty amounts of money. MSS aims to keep enterprises informed of potential cyberattacks by continuously monitoring cyber threats, enabling enterprises to opt for preventive measures efficiently.

Many small and medium-sized enterprises (SMEs) and large corporations are choosing cloud computing due to its benefits, including cost-effectiveness, dynamic access to data, and faster business processes. Cloud services offer security policy enforcement, various compliances, encryption, IAM, SIEM, and malware detection and prevention. This makes cloud computing an attractive option for businesses that want to have greater control over their data and infrastructure. These benefits have led to the increased adoption of cloud technology by SMEs and large enterprises, making it a cost-effective and efficient solution for these organizations. Additionally, managed security service providers can offer custom-based security solutions to enterprises that are looking to move their businesses to the cloud.

3.2.3.3 Rising demand for advanced cybersecurity measures

As Information technology continues to evolve and digitalization increases, cyberattacks are becoming more sophisticated and layered. Therefore, information and data security are crucial for the private and public sectors to protect against professional cybercriminals and advanced cyber threats. Cybercriminals use multi-layered cyberattacks to monitor individuals, enterprises, and nations for intelligence and commercial purposes. Therefore, organizations require comprehensive security services that can reduce costs while improving facility safety. Standalone security solutions are inadequate for addressing unified threats, and the costs associated with implementing and monitoring individual services present an additional challenge. As a result, there is an increasing demand for robust and cost-effective security services that can monitor and manage security events around the clock. This growing need is likely to drive growth in the overall services segment.

Next-generation cybersecurity measures, such as firewalls, IDS/IPS, and SIEM, provide advanced threat protection by integrating real-time contextual awareness, automated intelligent security, rapid response, and low cost of ownership. These next-generation security measures provide automatically prioritized network alerts, determine the cause of malware infection, and proactively protect servers and endpoints. They can also correlate various network topologies, threats, and reputation data. Therefore, to satisfy the increasing need for in-depth and continuous analysis of data across an organization and the ability to extract actionable intelligence from it, the demand for robust and cost-effective security services among enterprises is expected to drive the growth of the MSS market.

3.2.4 CHALLENGES

3.2.4.1 Balancing scalability with operational efficiency

Balancing scalability with operational efficiency is a critical challenge in the MSS market, particularly as client demands grow more complex and threat volumes continue to rise. As MSS providers onboard more clients and expand services across regions, ensuring consistent, high-quality protection becomes increasingly difficult. Scaling security operations involves expanding infrastructure and investing in skilled personnel, advanced analytics, and automation, each of which adds cost and complexity. According to ISACA's 2024 report, 62% of security leaders identify scalability limitations as a key barrier to effectively meeting enterprise security needs. Performance issues like delayed threat detection, prolonged incident response, and high rates of false positives can undermine client trust. Additionally, Managed Security Service Providers (MSSPs) that operate across diverse industries must tailor their services to different compliance requirements and risk profiles, which further strains their operational capacity. Without scalable, cloud-native Security Operation Centers (SOCs) and AI-driven threat management frameworks, these providers face the risk of bottlenecks and damage to their reputation. Therefore, scalability is a crucial factor for long-term sustainability in the market.

3.2.4.2 Rising cyberattacks on infrastructure of managed security service providers

Large enterprises regularly have structural difficulties that other smaller businesses typically do not experience. For instance, a broadly diverse customer base, numerous products & services offered worldwide, discrete internal divisions or hierarchical units, and essentially more outsourced business information are issues that large enterprises routinely face. Thus, it is challenging for large players in the MSS market to maintain and secure data to provide such security services. Providers are aware of threats, allocate resources toward information security, have faster response times, and offer recovery programs post-threat detection. To safeguard the security services of a provider's IT infrastructure against viruses, malware, and other cybersecurity threats, most vendors implement a unified strategy for managing security, which is a practical solution for growth-oriented companies.

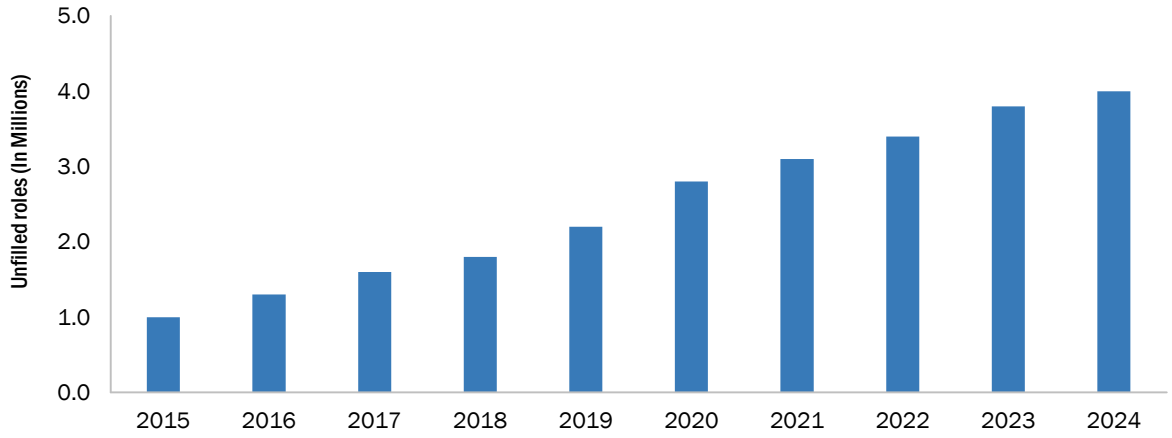
3.2.4.3 Shortage of security professionals

The managed security infrastructure is becoming more complex as technology advances. There are multiple ways for cyber threats to enter a virtual enterprise. Despite the increasing number of critical issues, only a limited number of trained professionals can comprehend and respond to sophisticated attacks. According to the 2024 (ISC)2 Cybersecurity Workforce Study, the global cybersecurity workforce has plateaued at around 5.5 million professionals, just a 0.1% growth from 2023, while the workforce gap has widened to approximately 4.8 million, marking a 19% year-over-year increase. Over two-thirds of organizations surveyed reported staff shortages, with 58% citing this as a major risk factor. Due to the severe shortage of qualified security personnel, organizations are exposed to serious risks. Cyber threats target network vulnerabilities and exploit them to infiltrate enterprise networks. With cyber-attacks on the rise, new zero-day threats have emerged. The methods and techniques utilized by attackers to breach an organization's enterprise network remain undetected.

According to the Australian Institute of Criminology, cybercrime is costing businesses in Australia around USD 1 billion annually. A Cybersecurity Workforce study by (ISC)2 found that the global cybersecurity industry is currently short by 4.8 million people, severely impacting organizations' ability to secure their complex information systems and networks. As shown below, the global cybersecurity workforce gap has grown significantly over the last decade. This rising shortfall in skilled professionals puts immense pressure on MSS providers to meet rising demand.

The graph highlights a four times increase in unfilled cybersecurity roles between 2015 and 2024.

FIGURE 5 GLOBAL CYBERSECURITY WORKFORCE GAP (2015-2024)



Source: isc2.org, weforum.org, and MarketsandMarkets Analysis

This widening skills gap poses a systemic risk to MSS providers. With fewer skilled analysts available in-house, organizations face slower detection and response times, increasing their dependency on outsourced MSS. MSS providers themselves also struggle to scale, as talent shortages limit the speed and quality of delivery service. Many organizations fail to allocate enough resources to their security infrastructure due to a lack of awareness of advanced cyber threats, leading to significant losses. In addition, companies with critical security needs experience a significant shortage of qualified professionals, making them more susceptible to cyberattacks and threats.

3.2.4.4 Limited capital funding in emerging economies

Limited capital funding can be a significant challenge for small and medium-sized companies that want to adopt the MSS model. Emerging start-ups in developing countries across the Middle East, Africa, Latin America, and the Asia Pacific often struggle to secure the necessary funding to implement MSS solutions for their business. These firms typically allocate most of their capital funding in safeguarding business-critical operations, leaving little to no funding for advanced security solutions. Additionally, cybersecurity budgets in emerging start-ups are often insufficient to implement firewall solutions, MDR solutions, SIEM, and log management solutions.

Limited funding and a lack of investments are expected to hinder the adoption of MSS among small firms in emerging economies. Due to financial constraints, these firms often lack proper IT security infrastructures, which results in a slow adoption of new technologies and enterprise security solutions. Small businesses struggle with managing their budgets for various operational challenges and business continuity planning, leaving less focus on adopting security solutions.

3.3 CASE STUDY ANALYSIS

In this case study analysis, we delve into the growing significance of MSS in the market by examining real-world examples and trends, resulting in many potential use cases. This section includes use cases from vendors providing MSS. Nevertheless, MSS applications are growing deep into BFSI, healthcare, retail, IT & ITeS, and government verticals.

3.3.1 NTT SECURES SYNTHOMER'S GLOBAL OPERATIONS WITH MANAGED SECURITY AND ADVANCED THREAT DETECTION

CLIENT	SYNTHOMER (UK)
Vendor	NTT DATA (Japan)
Description	Synthomer, a global leader in aqueous polymers, partnered with NTT DATA to enhance its cybersecurity infrastructure across 38 global sites. The collaboration standardizes firewall systems and leverages managed services for threat detection and network security.
Challenge	Synthomer needed complete visibility and consistent security across its global network, mainly post-acquisition of Omnova. Due to evolving cyber threats, a unified firewall infrastructure and standardized security policies were required to reduce risk and support business growth.
Solution	NTT DATA deployed Palo Alto Networks' firewall platform and provided global MSS, including advanced threat detection and centralized policy enforcement. Their global presence enabled rapid, seamless deployment across locations.
Benefit	Synthomer gained robust, scalable cybersecurity infrastructure, continuous threat intelligence, and agility to securely expand operations. The integrated approach improved visibility, user awareness, and communication across the organization, strengthening overall security posture.

Source: Company Website and Press Releases

3.3.2 VERIZON EMPOWERS FUJIFILM WITH 24/7 GLOBAL THREAT DETECTION THROUGH ADVANCED SOC SERVICES

CLIENT	FUJIFILM HOLDINGS CORPORATION (JAPAN)
Vendor	Verizon (US)
Description	FUJIFILM partnered with Verizon to strengthen its global cybersecurity monitoring using Verizon's Advanced Security Operations Center (SOC). This collaboration supports FUJIFILM's digital transformation by enabling centralized, 24/7 threat detection across its international operations.
Challenge	With 280 subsidiaries worldwide and a lack of unified security monitoring, FUJIFILM faced delays in detecting threats and responding to incidents. A rising volume of complex cyberattacks exposed weaknesses in their traditional infrastructure-focused surveillance systems.
Solution	FUJIFILM adopted Verizon's SOC services for continuous global threat monitoring, leveraging Verizon's expertise, advanced analytics, and SIEM capabilities. Verizon also helped Fujifilm analyze attacker traits and detect sophisticated attacks.
Benefit	FUJIFILM achieved round-the-clock global surveillance, rapid threat detection, and more coordinated incident response across regions. The partnership improved cybersecurity intelligence and laid the foundation for Fujifilm's own SOC aligned with zero-trust principles.

Source: Company Website and Press Releases

3.3.3 DXC TECHNOLOGY HELPED INAIL ENCOUNTER CYBER THREATS WITH AUTOMATION AND ML

CLIENT	INAIL (ITALY)
Vendor	DXC Technology (US)
Description	INAIL, a public insurance body, partnered with DXC Technology to enhance its cybersecurity posture amid rising phishing and malware threats. By integrating automation, machine learning, and threat intelligence into its SOC, INAIL improved threat detection and response capabilities.
Challenge	In the face of growing phishing attacks and highly sophisticated malware, INAIL is at the forefront of preventing data breaches. The company manages large amounts of personal information, making it a prime target for cybercriminals. To fight against such crime, INAIL decided to go further to ensure the organization is getting up-to-date threat intelligence and is equipped with automated analysis and machine learning capabilities.
Solution	DXC Technology runs INAIL's security operations center (SOC). It provides most of the group's security services and a wide range of services across the Enterprise Technology Stack, including cloud and IT outsourcing services.
Benefit	DXC Technology incorporated open-source intelligence sources combined with leading security software to collect information on cyber threats and integrate the data into INAIL's security workflow. This workflow optimizes lists of efficient and reliable IOCs and redistributes them to all security tools.

Source: Company Website and Press Releases

3.3.4 LUMEN TECHNOLOGIES HELPED NET PROTECTIONS SECURE ITS NETWORK

CLIENT	NET PROTECTIONS (JAPAN)
Vendor	Lumen Technologies (US)
Description	Net Protections, a leading BNPL service provider in Japan, partnered with Lumen Technologies to secure its growing digital payment infrastructure. Lumen delivered advanced managed services and cloud connectivity, ensuring 24/7 availability and robust protection for their mission-critical operations.
Challenge	Net Protections provides the BNPL (buy now, pay later) payment service called "NP Atobarai," which predominantly caters to e-commerce businesses. The number of users of this service is rapidly increasing. As of March 2021, about 76,000 merchants have adopted this service. The number of transactions has reached approximately 66 million per year, and the total transaction amount is over 430 billion yen per annum. Net Protections requires a mission-critical infrastructure that is operational 24 hours a day to service its clients in the given ecosystem.
Solution	▪ Lumen Edge Private Cloud ▪ Lumen Advanced Managed Services ▪ Lumen Cloud Connect solutions ▪ Lumen Internet Services
Benefit	Supported by Lumen's Advanced Managed Services, Net Protections' private cloud is a mission-critical platform designed to be up and running daily.

Source: Company Website and Press Releases

3.3.5 TRUSTWAVE HELPED AUGMEDIX PROTECT VITAL HEALTHCARE INFORMATION

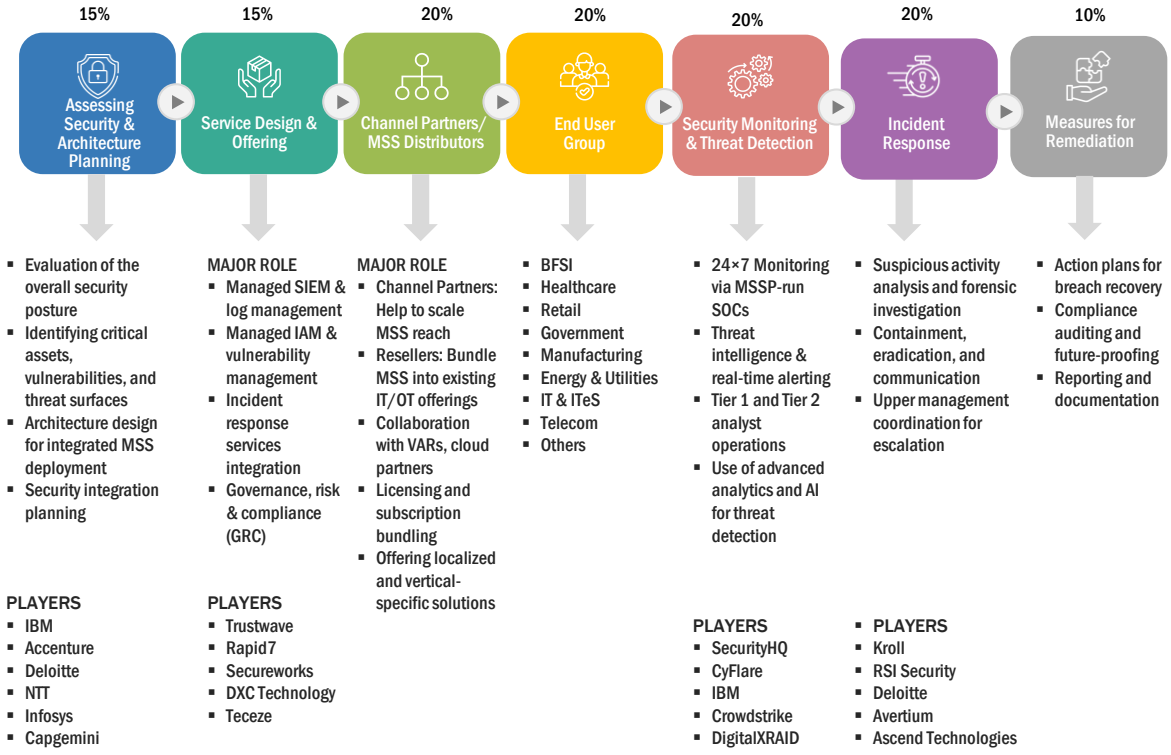
CLIENT	AUGMEDIX (US)
Vendor	Trustwave (US)
Description	Augmedix, a healthcare documentation provider, partnered with Trustwave after finding its previous SIEM solution inadequate. By onboarding to Trustwave's MDR platform, Augmedix strengthened the protection of sensitive health data and gained continuous visibility into its security posture.
Challenge	The company implemented a comprehensive security and risk management framework and added an SIEM tool provided by another security firm to accomplish this task, but found the product did not satisfy Augmedix's needs.
Solution	There was a complete process of onboarding Augmedix onto Trustwave's MDR platform that lasted about three months.
Benefit	With this solution, Augmedix can protect the extremely sensitive personal health information placed in its care by physicians and healthcare facilities. Also, through the Fusion platform and regular meetings with Trustwave account managers, Augmedix has a transparent and continuous look at its security status.

Source: Company Website and Press Releases

3.4 VALUE CHAIN ANALYSIS

The value chain for MSS outlines the key stages involved in delivering end-to-end cybersecurity solutions to organizations of all sizes. This structured framework encompasses proactive threat prevention, real-time monitoring, rapid incident response, and regulatory compliance. MSS providers play a critical role in extending specialized expertise and 24/7 protection for enterprises lacking in-house capabilities. The value chain ensures that security is not only reactive but also predictive and adaptive, helping organizations to stay ahead of an increasingly complex and evolving threat landscape.

FIGURE 6 MANAGED SECURITY SERVICES MARKET: VALUE CHAIN ANALYSIS



Source: Articles and MarketsandMarkets Analysis

The MSS market value chain outlines the sequential flow of activities and the key stakeholders that collectively ensure robust and continuous cybersecurity services. From initial assessment to post-incident remediation, each phase is vital in providing scalable, effective, and compliant security solutions to enterprises.

3.4.1 ASSESSING SECURITY & ARCHITECTURE PLANNING

This foundational stage evaluates an organization's existing security landscape and identifies vulnerabilities across networks, endpoints, and cloud assets. It defines the security posture, determines risk exposure, and aligns strategic objectives. MSSPs work closely with client leadership to validate architecture decisions and plan the integration of customized security controls. The output of this phase guides effective MSS deployment that is aligned with business operations. Key players in this phase include IBM, Accenture, Deloitte, NTT, Infosys, and Capgemini.

3.4.2 SERVICE DESIGN & OFFERING

At this stage, MSS providers define service bundles tailored to diverse enterprise needs. These typically include Managed Detection & Response (MDR), Managed Identity & Access Management (IAM), Vulnerability Management, Managed Firewall, Governance, Risk & Compliance (GRC), and SIEM & Log Management. Solutions may be offered as fully managed or co-managed, depending on client maturity and internal capabilities. Providers ensure service-level agreements (SLAs) and regulatory compliance requirements are embedded into the offering. This segment is served by Trustwave, Rapid7, Secureworks, DXC Technology, Teceze.

3.4.3 CHANNEL PARTNERS/MSS DISTRIBUTORS

Distributors, managed security resellers, and value-added resellers (VARs) serve as critical enablers in expanding market reach. They bridge the gap between MSSPs and customers in regional or vertical markets. These partners customize, package, and localize MSS offerings for sector-specific applications and compliance needs. Their role supports delivery efficiency, licensing, onboarding, and support services across industries.

3.4.4 END USER GROUP

MSS offerings serve a wide range of industry verticals such as BFSI, healthcare, retail, telecom, IT & ITeS, government, energy & utilities, and manufacturing. These organizations rely on MSS providers for 24/7 protection, secure remote operations, cloud threat monitoring, and compliance enforcement. SMEs benefit from outsourcing security management due to resource constraints, regulatory pressures, and increasing attack sophistication. The end user segment includes SMEs, large enterprises, and critical infrastructure providers.

3.4.5 SECURITY MONITORING & THREAT DETECTION

Continuous, real-time monitoring forms the backbone of MSS. Providers operate global or regional security operations centers (SOCs) where Tier 1 and Tier 2 analysts detect and triage threats. MSSPs leverage SIEM platforms, threat intelligence, machine learning, and behavioral analytics to identify anomalies and suspicious behavior. This phase enables rapid detection of threats and ensures system-wide visibility. Key players in this phase include SecurityHQ, CyFlare, IBM, CrowdStrike, and DigitalXRAID.

3.4.6 INCIDENT RESPONSE

This phase responds to and contains cybersecurity incidents. Analysts conduct root cause analysis, initiate containment protocols, and coordinate closely with client incident response teams and upper management. Investigations may involve digital forensics, malware analysis, and mitigation strategies to prevent lateral movement. A timely response is essential to minimize operational downtime and data exposure.

3.4.7 MEASURES FOR REMEDIATION

MSSPs guide clients through structured remediation plans to fix exploited vulnerabilities and reinforce defenses. Activities include patching, documentation, compliance audits, and risk assessments. Providers also help establish preventive controls to avoid recurrence. This stage ensures regulatory alignment and strengthens the client's long-term cybersecurity posture.

3.5 ECOSYSTEM ANALYSIS

The managed security services (MSS) market ecosystem is a diverse and interconnected landscape that brings together specialized providers addressing different facets of cybersecurity. It includes managed identity and access management providers, who ensure secure authentication and governance of user access; managed vulnerability management providers, who proactively identify and remediate system weaknesses; managed detection and response providers, who deliver continuous monitoring and rapid threat containment; managed risk and compliance management providers, who help organizations align with regulatory requirements and mitigate governance risks; and managed SIEM and log management providers, who centralize security data for advanced analytics and incident investigation. Collectively, these players form a robust ecosystem that enables organizations to strengthen their security posture, reduce operational burdens, and stay resilient against evolving cyber threats.

FIGURE 7 MANAGED SECURITY SERVICES MARKET ECOSYSTEM

Note: The above list is not exhaustive and is derived on the best effort basis

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 3 ROLE OF PLAYERS IN MANAGED SECURITY SERVICES ECOSYSTEM

COMPANY NAME	ROLE IN THE ECOSYSTEM
IBM (US)	Managed IAM, Vulnerability Management, MDR, SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall
NTT (Japan)	Managed IAM, Vulnerability Management, MDR, SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall
LevelBlue (US)	Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management
Accenture (Ireland)	Managed Endpoint Security, Managed Application Security, and Managed Cloud Security

DXC Technologies (US)	Managed IAM, Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall
Secnap US)	MDR, Managed SIEM & Log Management, Managed Firewall
Deloitte (UK)	Managed IAM, Managed Vulnerability Management, MDR, Managed Risk & Compliance Management, Managed SIEM & Log Management
Secureworks (US)	Managed IAM, Vulnerability Management, MDR, SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall, Security Monitoring
Trustwave (US)	Managed SIEM, Managed IAM, Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall
Verizon (US)	Managed IAM, Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall
Fujitsu (Japan)	Identity & Access Management and Vulnerability Management
HPE (US)	Managed IAM, Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Firewall
TCS (India)	Managed IAM, Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall
Atos (France)	Managed IAM, Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall, Security Monitoring
Orange Cyberdefense (France)	Managed Risk & Compliance Management, MDR, Managed SIEM & Log Management, Managed Firewall, Managed Vulnerability Management
Rapid7 (US)	Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed IAM
TrendMicro (Japan)	Managed SIEM & Log Management, MDR, Managed Firewall, Managed Vulnerability Management
Kudelski Security (Switzerland)	Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management
CrowdStrike (US)	MDR, Managed SIEM & Log Management, Managed Vulnerability Management
F5 (US)	Managed Firewall, MDR, Managed SIEM & Log Management
Capgemini (France)	Managed IAM, Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall
Infosys (India)	Managed Identity & Access Management (IAM), Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall.
Lumen Technologies (US)	Managed IAM, Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall
Kroll (US)	Managed IAM, MDR, Managed Risk & Compliance Management
Netsurion (US)	Managed Risk & Compliance Management, Managed SIEM & Log Management, MDR, Managed Firewall
Atlas Systems (US)	MDR, Managed Firewall, Managed SIEM & Log Management

Cipher (US)	Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed IAM
RSI Security (US)	Managed Risk & Compliance Management, Managed SIEM & Log Management, Managed Vulnerability Management
SecurityHQ (India)	Managed Vulnerability Management, MDR, Managed SIEM & Log Management, Managed Firewall, Managed Risk & Compliance Management
LightedgeH (US)	Managed SIEM & Log Management, Managed Firewall, MDR
LRQA (UK)	Managed Risk & Compliance Management, MDR
Teceze (UK)	Managed SIEM & Log Management, MDR
CyFlare (US)	Managed SIEM & Log Management, Managed Firewall, MDR, Managed Vulnerability Management
Ascend Technologies (US)	Managed Risk & Compliance Management, Managed SIEM & Log Management, MDR
Avertium (US)	Managed Risk & Compliance Management, MDR, Managed Firewall, Managed SIEM & Log Management, Managed IAM
DigitalXRAID (UK)	MDR, Managed Firewall, Managed SIEM & Log Management, Vulnerability Management, Managed Risk & Compliance Management
Trustnet (US)	Managed SIEM & Log Management, Managed Risk & Compliance Management, Managed Firewall, MDR, Vulnerability Management

Source: Company Websites, Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.6 IMPACT OF GENERATIVE AI ON MANAGED SECURITY SERVICES MARKET

3.6.1 GENERATIVE AI

Generative AI (GenAI) is a branch of artificial intelligence that produces original content and data. It is transforming industries by streamlining creative workflows, boosting analytical capabilities, and introducing novel solutions. Its potential in the market is vast, fueled by its capacity to generate everything from text and images to audio and other data formats. Integrating generative AI into the MSS market is set to transform key areas, making document checks and biometric authentication more efficient, accurate, and user-friendly. Here are the top use cases and market potential for generative AI in the MSS market.

3.6.2 TOP USE CASES AND MARKET POTENTIAL IN MANAGED SECURITY SERVICES MARKET

1) 24/7 Threat Monitoring and Real-time Incident Response:

- AI-powered Security Operations Centers (SOCs): MSS providers are deploying AI and machine learning to continuously monitor large volumes of security telemetry, enabling real-time threat detection and automated incident triage. This improves threat response times and reduces alert fatigue.
- Proactive Threat Containment: Advanced MSS offerings now feature automated playbooks that can isolate compromised endpoints or block malicious traffic within seconds of detection, which is essential for minimizing the impact of breaches during fast-moving cyberattacks.

2) Cloud Security and Compliance Management:

- Multi-Cloud Threat Visibility: With enterprises increasingly adopting multi-cloud and hybrid environments, MSSPs offer centralized visibility and protection across AWS, Azure, GCP, and private clouds, helping organizations enforce uniform security policies.
- Continuous Compliance-as-a-Service: MSSPs assist businesses in maintaining compliance with evolving standards (e.g., GDPR, HIPAA, PCI DSS) through automated audits, gap analysis, and real-time compliance monitoring dashboards.

3) Managed Detection and Response (MDR):

- Behavior-based Threat Detection: MSSPs are leveraging MDR services to analyze behavioral anomalies across endpoints, networks, and cloud workloads, identifying sophisticated threats such as lateral movement or insider attacks.
- Rapid Forensics and Threat Hunting: MDR allows MSSPs to perform deep forensic analysis and threat hunting across environments, closing the gap between detection and resolution while reducing dwell time.

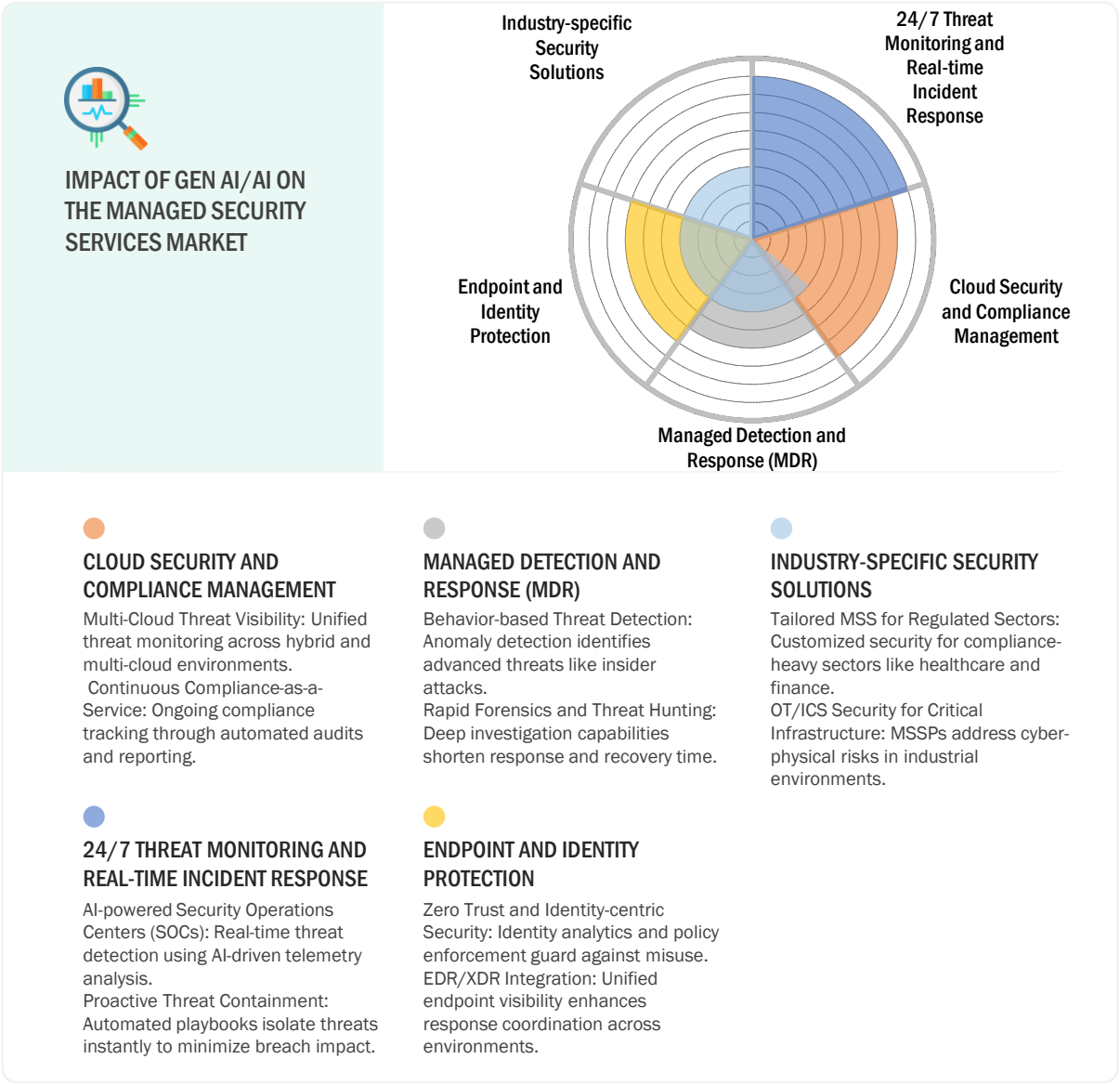
4) Endpoint and Identity Protection:

- Zero Trust and Identity-centric Security: MSSPs now offer identity protection services, including real-time user behavior analytics, privilege access management (PAM), and zero-trust policy enforcement to prevent identity-based breaches.
- EDR/XDR Integration: Integration with Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) platforms allows MSSPs to gain holistic visibility and coordinate responses across endpoints, applications, and users.

5) Industry-specific Security Solutions:

- Tailored MSS for Regulated Sectors: MSSPs are developing industry-specific solutions for healthcare, finance, manufacturing, and critical infrastructure, aligning with sectoral compliance requirements and threat landscapes.
- OT/ICS Security for Critical Infrastructure: MSSPs are expanding into operational technology (OT) and industrial control system (ICS) security, addressing a major gap in critical infrastructure protection against cyber-physical threats.

FIGURE 8 POTENTIAL OF GENERATIVE AI IN MANAGED SECURITY SERVICES MARKET ACROSS INDUSTRIES

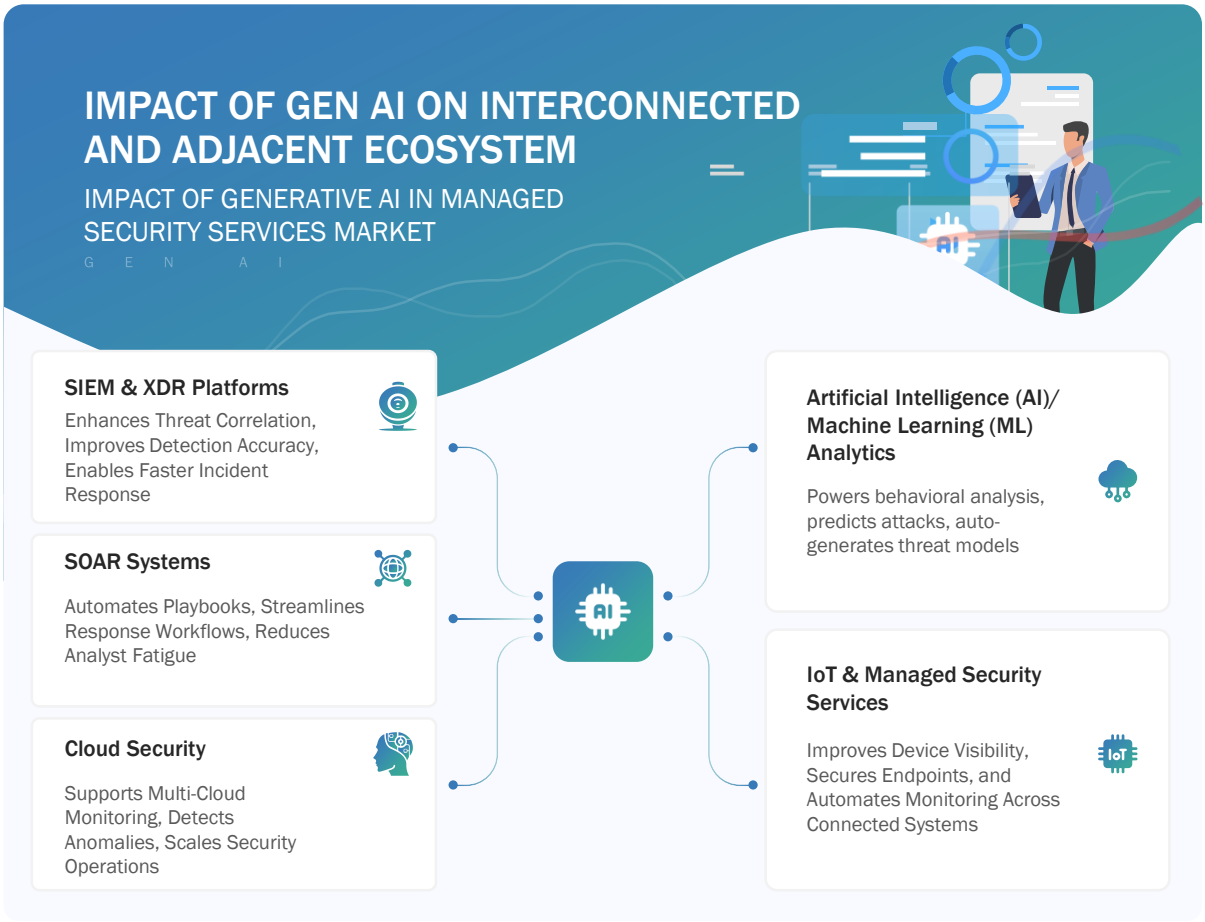


Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.6.3 IMPACT OF GENERATIVE AI ON INTERCONNECTED AND ADJACENT ECOSYSTEMS

Generative AI is transforming the MSS landscape by integrating with SIEM, XDR, IoT & MSS, and SOAR systems. It enhances threat detection through synthetic data modeling and enables faster, automated incident response. GenAI also strengthens predictive capabilities across cloud, IoT, and hybrid environments. This interconnected impact boosts scalability and resilience across banking and finance, healthcare, energy, retail, and government industries.

FIGURE 9 IMPACT OF GENERATIVE AI/AI ON INTERCONNECTED AND ADJACENT ECOSYSTEMS



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.6.3.1 SIEM & XDR Platforms

- Improved Threat Correlation: GenAI enhances SIEM/XDR engines by correlating disparate data sources and generating context-aware alerts, reducing noise and missed threats.
- Predictive Detection: AI models simulate advanced threats, helping systems anticipate and respond to zero-day attacks more proactively.

3.6.3.2 Soar Systems

- Automated Playbook Generation: GenAI builds dynamic incident response playbooks based on evolving threat scenarios, improving incident handling speed.
- Intelligent Workflow Tuning: It analyzes past responses to optimize and personalize response workflows for specific enterprise environments.

3.6.3.3 Cloud Security

- Anomaly Detection: GenAI enhances threat detection in multi-cloud setups, identifying behavioral outliers and potential breaches.
- Secure Data Handling: AI improves encryption workflows, data classification, and access control in distributed cloud environments.

3.6.3.4 Artificial Intelligence (AI)/Machine Learning (ML) Analytics

- Threat Simulation & Training: GenAI generates realistic attack patterns to train models and test MSS defenses.
- Adaptive Defense Mechanisms: It dynamically refines detection models based on threat evolution and client-specific environments.

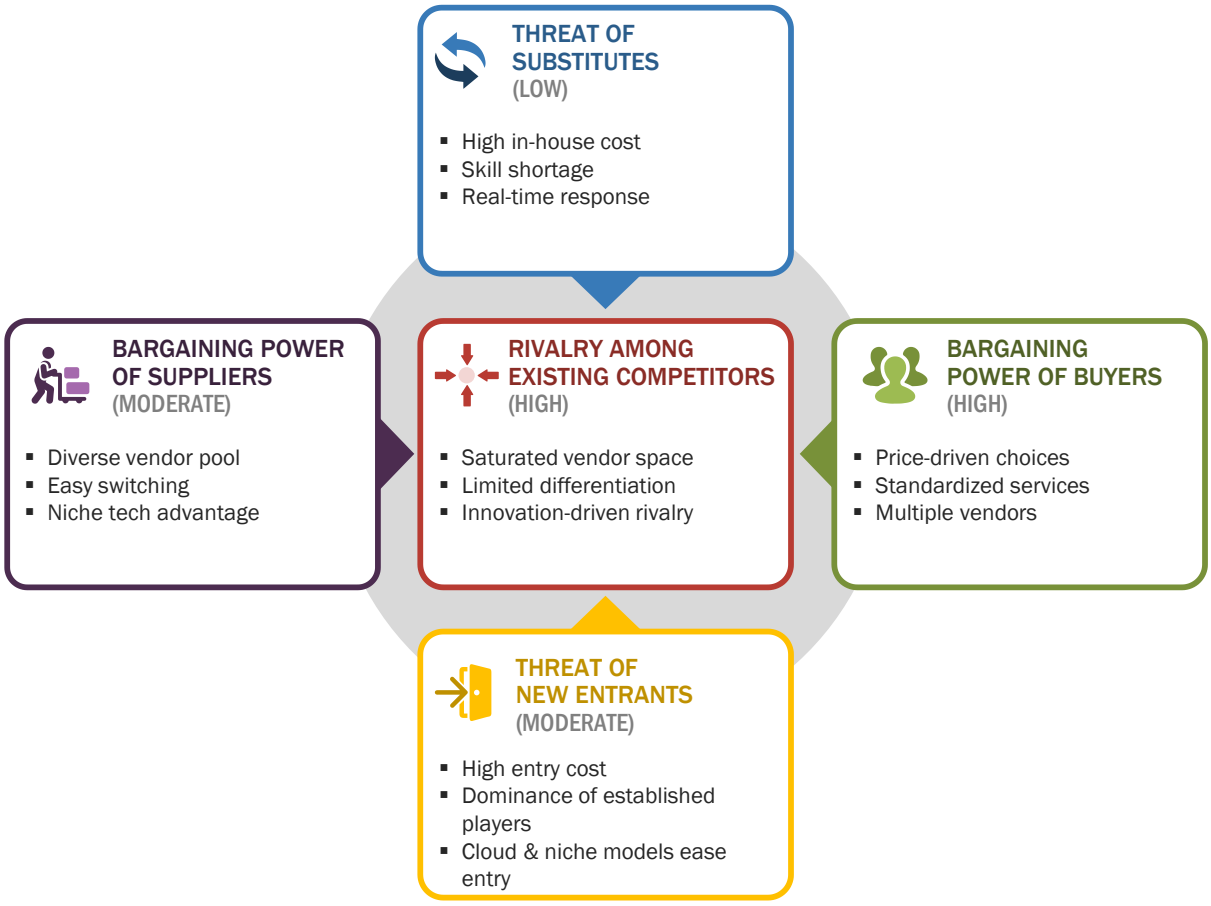
3.6.3.5 IoT & Managed Security Services

- Device Behavior Modeling: GenAI models typical IoT device behavior to flag irregularities and detect lateral movement early.
- Scalable Endpoint Monitoring: It enables MSSPs to manage vast numbers of endpoints by prioritizing high-risk activity in real-time.

3.7 PORTER'S FIVE FORCES ANALYSIS

Porter's five forces analysis is a framework that determines the competitive intensity of a market. This section analyzes the MSS market from five different perspectives: intensity of competitive rivalry within the industry, the threat of new entrants, the bargaining power of suppliers, the bargaining power of buyers, and the threat of substitutes. The following figure represents the analysis of Porter's five forces for the global MSS market.

FIGURE 10 MANAGED SECURITY SERVICES MARKET: PORTER'S FIVE FORCES ANALYSIS



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 4 PORTER'S FIVE FORCES' IMPACT ON MANAGED SECURITY SERVICES MARKET

PORTER'S FIVE FORCES	IMPACT
Threat of New Entrants	Moderate
Bargaining Power of Suppliers	Moderate
Bargaining Power of Buyers	High
Threat of Substitutes	Low
Intensity of Competitive Rivalry	High

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.7.1 THREAT OF NEW ENTRANTS

The threat of new entrants is the likelihood of new competitors entering a market and acquiring a market share that existing companies already hold. Establishing a competitive MSS operation requires significant investment in secure data centers, advanced tools, threat intelligence platforms, and skilled cybersecurity personnel. This high initial cost acts as a barrier for many potential entrants, particularly startups with limited funding.

The market is dominated by well-established companies with robust service portfolios, advanced R&D capabilities, and strong brand trust. These incumbents maintain deep client relationships and often have long-term contracts, making it difficult for newcomers to win market share quickly. Compliance is necessitated by regulatory landscapes, such as GDPR, HIPAA, and state-level US laws. New entrants must navigate these complex regulations and ensure their solutions are compliant from the start. Additionally, proprietary technologies and patented solutions create IP barriers that prevent easy replication of services.

Despite high entry barriers, the growing demand for MSS and the rise of cloud-based delivery models moderately lower the threat of new entrants by enabling startups and niche vendors to enter through partnerships and specialized offerings.

Hence, the threat of new entrants is moderate in the MSS market.

3.7.2 THREAT OF SUBSTITUTES

The threat of substitutes arises when customers can achieve similar results using alternative products, solutions, or services instead of those offered in the market. Many organizations, particularly small and medium-sized enterprises (SMEs), struggle to establish in-house security operations due to the high costs and complexities involved. Setting up a fully functional Security Operations Center (SOC), acquiring advanced tools, and maintaining 24/7 monitoring can be financially and operationally unfeasible for them. Additionally, there is a global shortage of cybersecurity professionals, making it challenging for organizations to effectively staff and manage an internal security team. Managed Security Service (MSS) providers address this gap by offering skilled experts and established processes.

Cyber threats are dynamic and require constant monitoring, intelligence sharing, and quick response. Managed security providers specialize in these areas and leverage AI/ML technologies for real-time detection and remediation. For most enterprises, maintaining this level of security sophistication internally is not feasible, making MSS offerings irreplaceable in practice.

Thus, the threat of substitutes is low in the MSS market.

3.7.3 BARGAINING POWER OF SUPPLIERS

Suppliers' bargaining power refers to suppliers' influence over the prices of components. They can achieve this by using the unique features of their products or by applying pressure on buyers. This pressure can manifest as increased prices, decreased quality, or reduced product availability. The MSS market benefits from a wide range of security hardware and software vendors offering similar products and services. This diversity reduces dependency on any single supplier, giving MSS providers the flexibility to switch vendors or negotiate better terms. The increased use of standardized cybersecurity frameworks and cloud-native security platforms lowers switching costs. Many MSS providers can integrate widely available cloud tools, which minimizes reliance on proprietary systems and weakens suppliers' leverage.

In contrast, suppliers offering niche technologies such as advanced threat intelligence feeds, proprietary AI/ML tools, or zero-day threat detection capabilities maintain a stronger influence. MSSPs relying on such specialized solutions may face higher costs or integration challenges if switching is attempted. Additionally, a growing trend of consolidation among security solution vendors can strengthen supplier power. If a few large tech firms dominate the security stack, MSSPs may have reduced room to negotiate for advanced analytics, automation tools, or premium licenses.

Hence, the bargaining power of suppliers is moderate in the MSS market.

3.7.4 BARGAINING POWER OF BUYERS

The bargaining power of buyers refers to their ability to influence the prices of products in a market. The presence of numerous MSS providers, both organized and unorganized, gives buyers multiple options. Many vendors offer similar service portfolios at different price points, making it easier for buyers to compare and switch providers, especially in price-sensitive markets. Also, as core MSS offerings such as threat monitoring, vulnerability management, and endpoint protection become standardized across vendors, buyers gain more leverage in negotiations. This service overlap reduces vendor lock-in and strengthens buyer power.

The MSS market in Asia Pacific and Latin America is highly price-driven. Buyers in these regions often prioritize cost over differentiation, compelling providers to lower prices or add value to remain competitive, thus elevating buyer influence.

Thus, the bargaining power of buyers is high in the MSS market.

3.7.5 INTENSITY OF COMPETITIVE RIVALRY

The competitive rivalry refers to the pressure that market players add on each other. The market is dominated by several well-established global players such as IBM, Accenture, Fujitsu, AT&T, Verizon, TCS, Atos, and DXC. These companies possess extensive service portfolios, long-standing industry experience, and strong customer relationships. Their widespread presence across regions indicates they aggressively compete for enterprise clients, creating sustained pressure on each other.

The strategic alliances and partnerships these players maintain with technology providers, cloud hyperscalers, and regulatory bodies enable them to offer bundled services with enhanced capabilities, raising the competitive bar and forcing other vendors to invest more heavily to keep up. Moreover, service differentiation is increasingly difficult in the MSS space. Threat monitoring, compliance management, and incident response are becoming standardized in this market, forcing vendors to compete on value-added services such as AI-based threat detection, faster response times, and better user experience. Additionally, the rapid pace of technological change with the rise of AI, zero-trust architecture, and hybrid cloud environments adds to the pressure. Vendors that cannot innovate quickly or adapt to clients risk losing relevance, making the market highly aggressive and innovation-driven.

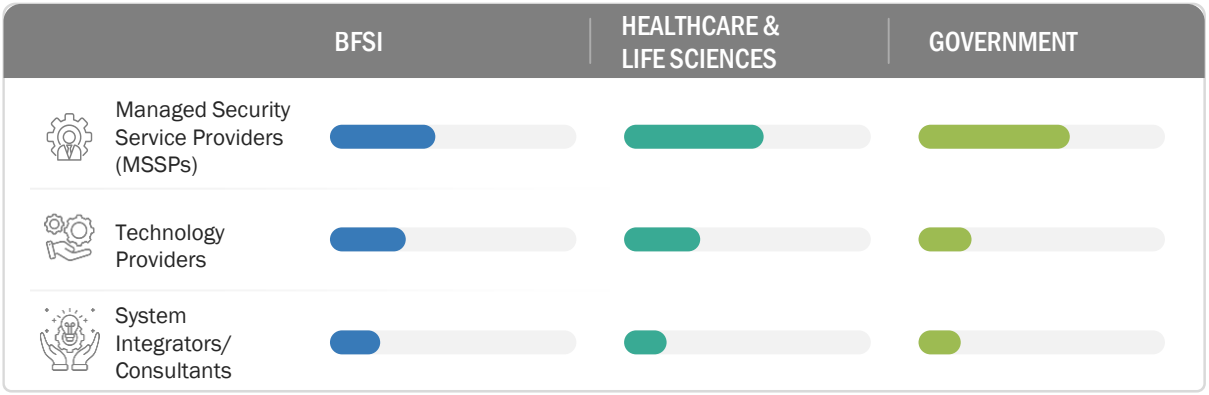
Thus, the intensity of competitive rivalry is high in the MSS market.

3.8 KEY STAKEHOLDERS AND BUYING CRITERIA

This section explains the key stakeholders and their influence on the buying process for each vertical.

3.8.1 KEY STAKEHOLDERS IN BUYING PROCESS

FIGURE 11 INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS



Source: Primary Research, Secondary Research, and MarketsandMarkets Analysis

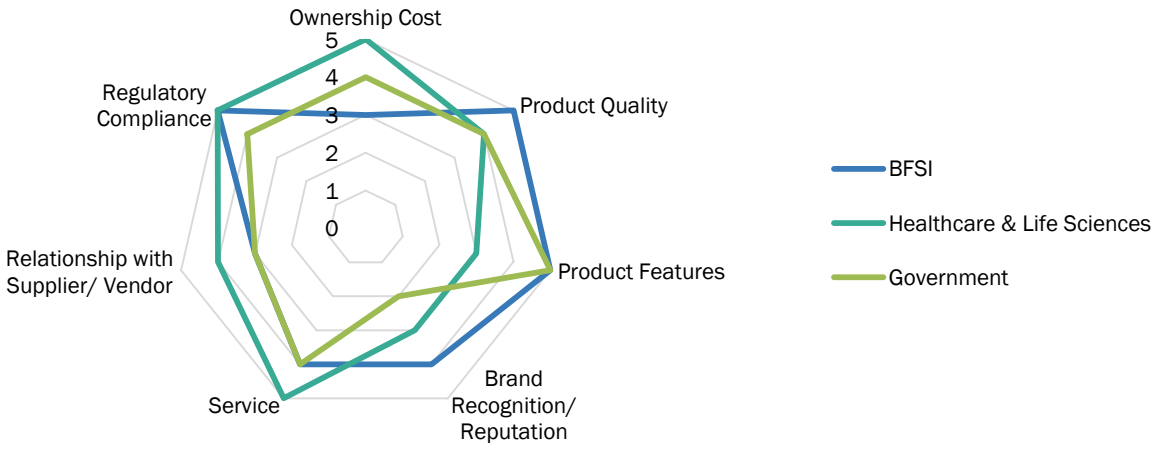
TABLE 5 IMPACT OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS

Key Stakeholders	BFSI	Healthcare & Life Sciences	Government
Managed Security Service Providers (MSSP's)	45%	50%	55%
Technology Providers	30%	30%	25%
System Integrators/Consultants	25%	20%	20%
Total	**100%**	**100%**	**100%**

Source: Primary Research, Secondary Research, and MarketsandMarkets Analysis

3.8.2 BUYING CRITERIA

FIGURE 12 KEY BUYING CRITERIA FOR TOP THREE VERTICALS



Source: Primary Research, Secondary Research, and MarketsandMarkets Analysis

TABLE 6 KEY BUYING CRITERIA FOR TOP THREE VERTICALS

Buying Criteria	BFSI	Healthcare & Life Sciences	Government
Ownership Costs	3	5	4
Product Quality	5	4	4
Product Features	5	3	5
Brand Recognition/Reputation	4	3	2
Services	4	5	4
Relationship with Suppliers/Vendors	3	4	3
Regulatory Compliance	5	5	4

Source: Primary Research, Secondary Research, and MarketsandMarkets Analysis

3.9 PRICING ANALYSIS

Pricing packages for MSS vary vastly, as various variables are involved, such as the number of users, type of service, customizations required, size of the organization, and deployment type. MSS vendors provide various pricing models, including options based on the number of users, monthly fees, and annual subscriptions. These vendors also offer scalability, meaning that pricing increases as the number of users grows. Additionally, there are a variety of add-ons available to meet specific customer needs. The monthly subscription rate can vary as several providers may cost from USD 20 to USD 2000 based on capabilities and the number of users.

However, the subscription price is only one component of the overall cost. Customizations, integrations, and consulting can dramatically increase the overall price. The pricing will depend on and vary with multiple factors, such as the number of users, the type of service, add-ons required, and the level of support. The managed service vendors can charge users with different pricing models such as monitoring only, per device, per user, fixed, tiered, and A La Carte. These models are as follows:

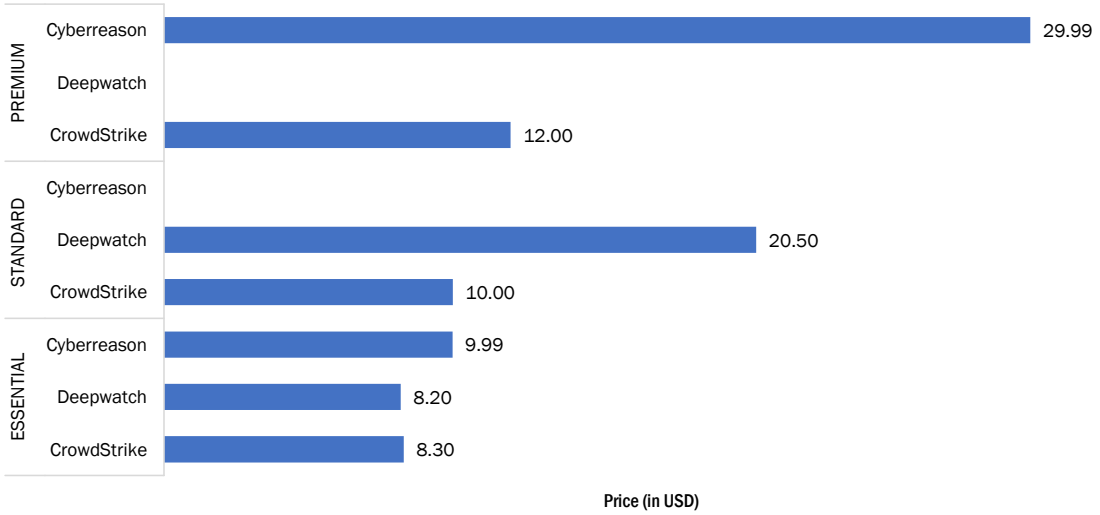
- Monitoring Only: It provides network monitoring and alerting services. Users can accommodate different service levels. These services are generally feasible for SMEs and medium-sized organizations with budget constraints.
- Per Device: Per device is a pricing model where organizations are charged per device as they opt for MSS. The pricing is fixed for each device and modified as customers add new devices.
- Per User: The per-user pricing model is similar to a per-device pricing model, with the only difference being that managed security service providers charge a flat fee per user per month instead of per device. It covers all the end-user devices.
- Tiered: The tiered pricing model refers to the model where managed security service providers offer different tiers of bundled service packages. The pricing is dynamic and increases from tier to tier as the set of services increases.
- Fixed: The fixed pricing model offers fixed service packages for a fixed amount. Users can use those services as much as they want in the billing cycle. These services cover all remote and on-site support and are charged per month.
- Flat-free: With a flat-free pricing model, organizations can access various services, including remote and on-site support, without the need to recalculate their monthly budget.
- A La Carte: A La Carte service refers to a pool of services offered at different rates. Organizations can choose the required services from these pools of services and pay for only those they use. These services offer high customization to clients and cater to various tailor-made solutions.

- Customized/Outcome-based: The customized/outcome-based pricing model is based on business risk, compliance requirements, or specific outcomes, such as reduced dwell time or breach prevention.
- Event/Log Volume-based: Event/log volume-based pricing charges are based on the volume of security logs or events processed (e.g., GBs/day or events per second). This pricing model is commonly adopted for SIEM-as-a-service or SOC monitoring.

3.9.1 AVERAGE SELLING PRICE OFFERED BY KEY PLAYERS, BY TYPE, 2024

The pricing landscape for MSS offerings in 2024 highlights clear differentiation across service tiers. Cybereason positions itself as a premium leader with the highest price point at USD 29.99, while CrowdStrike offers more affordable options across all tiers. Deepwatch emerges strong in the standard segment with USD 20.50, reflecting its mid-tier focus. In the essential tier, pricing remains closely aligned, with all players ranging between USD 8.20 and USD 9.99, indicating strong competition for cost-sensitive customers. Overall, the trend underscores a tier-based pricing strategy tailored to diverse customer segments.

FIGURE 13 AVERAGE SELLING PRICE OFFERED BY KEY PLAYERS, BY TYPE, 2024



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 7 AVERAGE SELLING PRICE OFFERED BY KEY PLAYERS, BY TYPE, 2024

Type	Essential	Standard	Premium
CrowdStrike – Falcon Complete MDR	USD 8.30/user/month	USD 10.00/user/month	USD 12.00/user/month
Deepwatch – MEDR/MDR	USD 8.20/device/month (MEDR)	USD 20.50/device/month (MDR)	NA
Cyberreason – MDR	USD 9.99/user/month	NA	USD 29.99/user/month

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.9.2 INDICATIVE PRICING ANALYSIS, 2024

MSS providers offer a range of pricing structures, each designed to accommodate diverse business needs and preferences. From user and device-based models to tiered service levels and risk-based pricing, these approaches provide flexibility and scalability to organizations of varying sizes and industries. In this exploration of indicative pricing models for MSS, we delve into the key considerations that shape these models, empowering businesses to make informed decisions in aligning their cybersecurity strategy with budgetary constraints and specific security requirements.

A few pricing models are listed below:

- Per-user Pricing: This model charges a fixed fee per user connected to the network or protected by the MSS service. It is simple to understand and scales easily with your organization's size.
- Indicative Cost: USD 50–USD 200 per user per month
- Per-device Pricing: This model charges based on the number of devices (endpoints, servers, network devices) covered by the MSS service. It suits organizations with diverse device types.
- Indicative Cost: USD 10–USD 50 per device per month
- Tiered Pricing: This model offers different service tiers with varying features and functionalities, allowing you to select a plan that aligns with your specific needs and budget.
- Indicative Cost: Tier 1 – Basic (limited features): USD 1,000–USD 5,000 per month; Tier 2 – Advanced (increased features): USD 5,000–USD 15,000 per month; Tier 3 – Premium (comprehensive services): USD 15,000+ per month
- Pay-as-you-go: This model offers flexibility by charging only for the specific services you use and the amount of data you generate. It suits organizations with fluctuating security needs.
- Indicative Cost: Varies depending on service usage and data volume
- Retainer-based Pricing (for IR services): In this model, clients pay a fixed monthly fee to retain access to MSSP's expert response team, which is used for proactive or emergency incident response.
- Indicative Cost: USD 5,000–USD 25,000/month based on response SLAs and threat landscape

TABLE 8 INDICATIVE PRICING LEVELS OF MANAGED SECURITY SERVICES VENDORS, 2024

COMPANY	PRODUCT	PRICING
CrowdStrike	▪ Falcon Prevent (Next-Gen Antivirus) ▪ Falcon Insight (EDR) ▪ Falcon OverWatch (MDR) ▪ Falcon Complete (Fully Managed MDR)	▪ Included in all plans: USD 59.99 to USD 184.99 per device/year ▪ Included from Pro plan upward: starts at ~USD 99.99 per device/year ▪ Included in Falcon Complete or as add-on: USD 12–16 per device/month ▪ Full-service MDR with remediation: USD 100–125 per endpoint/year
UnderDefense	▪ Managed SOC / SOCaaS	▪ USD 10–20 per asset/month across devices/users

Blueberry Security	▪ SOC-as-a-Service	▪ Starting with a range of USD 10–20/device/month (typically USD 10/device/month) ▪ Penetration Testing Services: USD 120/hr ▪ Phishing training: USD 10/user/month) ▪ Cyber Security Consulting: USD 100/hr
Collabrance	▪ NOC Services	▪ USD 13 per workstation per month ▪ USD 60 per server per month
Trustnet	▪ Essential ▪ Pro ▪ Select ▪ Prime	▪ USD 2,275/ month ▪ USD 2,375/ month ▪ USD 2,625/ month ▪ USD 4,775/ month
N-Able	▪ Per-Device	▪ USD 69 per desktop ▪ USD 299 per server ▪ USD 29 per network printer ▪ USD 99 per managed network
Alibaba Cloud	▪ MDR	▪ USD 1800/month
Trilight Security	▪ SMB ▪ Managed security services	▪ USD 6.48/user/month ▪ USD 8.64/user/month
CyberSecOp	▪ Per-Device Pricing or Per-User Pricing	▪ Range from USD 10 to USD 200 or USD 64 to USD 250 per user monthly
CP Cyber	▪ SOC Staffing	▪ USD 2,310,000–USD 4,620,000 for 3 years

Note: The prices may or may not involve administration and support costs and are subject to change depending on the number of users, company requirements, and comprehensiveness of solutions.

Benefits include features provided with the highest tier of MSS.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.10 TECHNOLOGY ANALYSIS

The MSS market's technological landscape is advancing quickly due to the integration of AI and ML, which enhances the effectiveness and precision of managed security processes. These technologies enable proactive threat detection, anomaly analysis, and rapid incident response, helping businesses prevent identity-based attack vectors and unauthorized access. Cloud-based MSS are gaining momentum due to their scalability and cost-effectiveness, enabling enterprises, mainly SMEs, to deploy robust protection without the need for extensive infrastructure or budgets. Moreover, the industry is evolving with the integration of blockchain technology, which introduces a decentralized model for event logging and identity management, potentially revolutionizing the way organizations secure and audit digital environments.

Furthermore, the market is transforming by introducing multimodal biometric solutions that combine various biological traits for verification, amplifying security measures beyond single-point identification systems. Complementary technologies such as Threat Intelligence Platforms (TIPs) and Identity Threat Detection and Response (ITDR) are also being widely integrated to strengthen authentication layers, monitor behavioral deviations, and secure edge environments. The combination of these technologies shapes a more secure, efficient, and user-friendly landscape for MSS across many sectors.

3.10.1 KEY TECHNOLOGIES

3.10.1.1 AI/ML and managed security services

Artificial intelligence (AI) is a branch of computer science that deals with building machines that can perform tasks related to human intelligence, like problem-solving, reasoning, and analysis. It has transformed the way data is interpreted and analyzed. AI collects information from various resources and enables the management to derive results from the collated data. AI can assist managed service providers with automated solutions to business requests. It can also help clients in deciding the best fit for their organization and enrich alerts with contextual intelligence. Machine learning (ML) is a branch of artificial intelligence that supports businesses by extracting insights from raw data and solving complex business problems. It can be beneficial in the managed service domain as it continuously learns from historical incidents to improve threat detection accuracy. ML can leverage predictive analytics for real-time insights and enhance the customer experience for vendors. This shift from reactive to predictive cybersecurity is helping organizations minimize response times and reduce the burden on their security teams.

Darktrace is at the forefront of this evolution. Its AI-powered Antigena platform includes numerous advanced machine learning models designed to autonomously respond to threats as they unfold. Antigena acts as a digital immune system, making thousands of decisions per second to contain threats such as ransomware, insider breaches, or lateral movement within networks—without the need for manual intervention. Similarly, CrowdStrike has integrated ML into its Falcon platform to provide endpoint protection that evolves with new threat vectors, while IBM uses AI-driven analytics in QRadar to prioritize incidents based on severity and business risk.

These real-world applications of AI and ML highlight how MSS providers are transforming cybersecurity from a manual, reactive task into an intelligent, autonomous process. By embedding learning algorithms and adaptive intelligence into their security operations, vendors can offer clients faster, more accurate, and scalable protection across increasingly complex digital environments.

3.10.1.2 Cloud-based security solutions

The landscape of cloud-based security solutions is ever-evolving, addressing dynamic challenges in innovative ways. Key trends include an increased focus on securing cloud-native environments, with dedicated platforms for Kubernetes and serverless architectures. Platforms tailored for Kubernetes and serverless architectures are now essential, as attackers increasingly target these areas. Cloud-native Application Protection Platforms (CNAPPs) enriched with AI/ML can reduce incident detection time from an average of 16 days to just 10 minutes, while zero trust and enhanced encryption safeguards ensure robust inter-service and API protection.

Advancements in AI/ML-driven threat detection and Security Orchestration, Automation, and Response (SOAR) streamline operations, while multi-cloud security management emphasizes unified visibility and cloud-agnostic tools. Artificial Intelligence and Machine Learning are embedded throughout cloud security, powering real-time anomaly detection, automated compliance, and proactive risk management. Around 94% of organizations use generative AI apps, prompting the adoption of AI-driven DLP and Cloud Security Posture Management (CSPM) solutions to control data flows. Data security and compliance see improvements in DLP and automated compliance, and the emergence of Security-as-a-Code (SaC) introduces IaC scanning and DevSecOps automation. Collectively, these trends signify a robust and efficient era in cloud security.

3.10.1.3 Security information and event management

Security Information and Event Management (SIEM) is a technology that acts as a centralized platform for real-time threat detection, incident response, and regulatory compliance. SIEM tools collect, aggregate, and normalize logs and security data from across an organization's IT environment, including endpoints, servers, applications, and network devices, providing a unified view of security events. By leveraging advanced analytics, machine learning, and correlation rules, SIEM enables MSS providers to detect anomalies, flag potential breaches, and identify patterns of malicious activity. This proactive monitoring is essential in a modern threat landscape where attacks are often subtle, multi-stage, and difficult to detect through siloed tools.

Major MSS providers have integrated SIEM deeply into their security operations. For example, IBM uses its QRadar SIEM platform to deliver managed threat detection and response services to large enterprises, offering automated analysis of billions of events per day. Splunk's SIEM, often paired with its analytics and dashboard capabilities, is widely adopted by financial institutions for fraud detection and log monitoring. Healthcare provider Ascension uses LogRhythm's SIEM solution to meet HIPAA compliance while gaining centralized visibility across several locations. These examples highlight how real-world organizations rely on SIEM as a strategic asset to enhance their security posture and regulatory readiness.

SIEM platforms enable MSS providers and enterprise clients to unify their security data, detect, and respond to threats in real time and maintain compliance with evolving regulations.

3.10.1.4 Security orchestration, automation, and response

Security Orchestration, Automation, and Response (SOAR) offers a robust solution to the rising volume and complexity of security alerts. Unlike traditional manual processes, SOAR platforms allow MSS providers to automate incident triage, contextualize alerts with real-time intelligence, and trigger predefined response playbooks. This automation accelerates response times and ensures consistency in handling threats across distributed environments. For example, Palo Alto Networks' Cortex XSOAR allows organizations to define detailed playbooks for use cases such as phishing, ransomware, or insider threats, reducing response time from hours to minutes. By automating repetitive, low-level tasks, SOAR frees up human analysts to focus on strategic threat hunting and investigation.

Several enterprises have adopted SOAR solutions to enhance the efficiency of their security operations centers (SOCs). IBM's QRadar SOAR, used in conjunction with its SIEM, has been deployed by large healthcare networks in the US to orchestrate complex incident response workflows while maintaining HIPAA compliance. Financial institutions, such as Barclays, use Splunk Phantom to automate their phishing investigation processes, allowing them to triage and remediate hundreds of suspicious emails daily with minimal analyst intervention. SOAR enhances MSS by enabling rapid, scalable, and automated threat response, helping Barclays and IBM clients to reduce detection and response times while optimizing the effectiveness of their security teams.

3.10.2 COMPLEMENTARY TECHNOLOGIES

3.10.2.1 Threat intelligence platforms

Threat Intelligence Platforms (TIPs) have become critical complementary technologies for MSS by enhancing the proactive capabilities of threat detection, prevention, and response. TIPs aggregate, analyze, and operationalize threat data from open-source intelligence, commercial feeds, industry-specific threat data, and internal telemetry, thus providing MSSPs with a centralized and contextual view of emerging threats. This intelligence is then used to enrich alerts from SIEM or XDR systems, prioritize incidents, and automate threat response workflows, which significantly reduces false positives and improves incident triage efficiency.

These platforms are complementary because, while core MSS technologies such as SIEM or SOAR handle event monitoring and response, TIPs add the strategic depth of external threat visibility. For instance, MSSPs can use TIPs to correlate external indicators of compromise (IOCs) with internal telemetry to detect stealthy or targeted attacks. Recorded Future, Anomali, and ThreatConnect offer enterprise-grade TIPs that integrate with MSS stacks. A recent example includes IBM integrating its X-Force Threat Intelligence into its MSS offerings to provide contextual, real-time threat insights across client environments. Similarly, Secureworks uses its TIP to continuously update detection logic for its Taegis XDR platform, proactively defending clients from evolving ransomware campaigns. Threat intelligence platforms enable MSS providers to move from reactive to predictive security operations by equipping them with timely and actionable threat intelligence that strengthens decision-making and accelerates response efforts.

3.10.2.2 Identity threat detection and response

Identity threat detection and response (ITDR) is a rapidly evolving technology that safeguards identity infrastructure such as Active Directory (AD), Azure AD, and identity providers such as Okta, Ping Identity, or Auth0. With identity becoming the new perimeter in a cloud-first and hybrid workforce environment, ITDR plays a critical role in detecting, investigating, and responding to identity-based threats that bypass traditional endpoint or network defenses.

ITDR solutions monitor for suspicious authentication patterns, privilege escalations, credential misuse, or lateral movement that often signal an identity compromise. They provide deep visibility into how identities are being accessed and manipulated, correlating this with threat intelligence and behavioral baselines. MSS providers are increasingly incorporating ITDR capabilities into their offerings to deliver identity-centric threat detection across customer environments.

Microsoft (through Defender for Identity), CrowdStrike (Falcon Identity Protection), and Semperis are at the forefront of ITDR deployment, offering enhanced visibility and control over identity infrastructures, bridging critical gaps left by traditional detection tools.

3.10.3 ADJACENT TECHNOLOGIES

3.10.3.1 Zero-trust architecture

The Zero Trust architecture (ZTA) landscape is a dynamic arena in the ongoing battle against cyber threats, witnessing exciting developments that redefine security paradigms. Cutting-edge implementations include container-level microsegmentation, enabling granular access controls that can isolate individual Kubernetes pods or workloads based on identity and context. Real-world adopters such as Google, through its BeyondCorp initiative, have fully embraced Zero Trust principles by enforcing continuous authentication and access control regardless of user location. Additionally, initiatives such as the U.S. Government's Executive Order 14028 are pushing agencies to adopt zero-trust frameworks, marrying enforcement with guidance from NIST and CISA. At the core of Zero Trust innovation lies the implementation of dynamic, real-time risk-based access controls that move beyond static, rule-based authorization models. Zero-Trust Network Access (ZTNA) solutions extend beyond secure remote access, unifying access controls across diverse environments. Modern ZTNA platforms continuously evaluate signals such as device posture, geolocation, and behavioral patterns to adjust permissions on the fly, automatically revoking access for anomalous users or devices when risk thresholds are exceeded.

Identity and Access Management (IAM) undergoes advancements with expanded multi-factor authentication options and the rise of passwordless solutions. For example, Twingate and Zscaler have rolled out solutions that provide seamless yet tightly controlled human-centric access beyond just traditional VPNs. To counter increasingly stealthy attacks, the Zero Trust ecosystem is also integrating deception technologies, deploying fake credentials and decoy assets that trigger alerts upon engagement. Collaboration between vendors and standards bodies such as NIST (SP 800-207, SP 1800-35) and CISA encourages interoperability, automation, and structured maturity paths for Zero Trust implementation.

These advancements collectively deliver a model where trust is never assumed but continually evaluated and enforced, providing robust protection against sophisticated threats.

3.10.3.2 IoT and managed security services

Managed security service providers (MSSPs) are increasingly playing a pivotal role in securing the expanding Internet of Things (IoT) ecosystem, offering end-to-end services that encompass device management, threat detection, data analytics, and compliance enforcement. As IoT deployments scale across industries from manufacturing to healthcare, MSSPs help enterprises monitor device behavior, detect anomalies, and maintain policy adherence across disparate endpoints. These services are particularly critical as IoT devices often lack built-in security capabilities, making them attractive entry points for threat actors.

Recent developments reveal a strong industry shift toward integrated IoT security platforms that blend operational technology (OT) visibility with IT-level intelligence. For example, Microsoft's Azure IoT Defender and Palo Alto Networks' IoT Security platform now integrate with broader MSS solutions, enabling continuous monitoring and behavioral analytics across connected devices. These tools empower MSSPs to deliver real-time threat mitigation, leveraging machine learning models to identify irregularities, isolate compromised endpoints, and initiate automated remediation workflows. Companies are forging partnerships to strengthen their IoT security edge. A notable example is Dell Technologies' continued collaboration with Litmus, which has now expanded to include broader orchestration across hybrid environments and edge-cloud integrations. Together, they provide a secure framework for managing industrial IoT (IIoT) data from manufacturing floors to enterprise applications. This demonstrates how MSSPs are becoming integral to IoT success by not only protecting infrastructure but also enabling scalable, secure innovation across connected ecosystems.

3.10.3.3 Extended and detection response

Extended detection and response (XDR) continues to redefine enterprise security operations by centralizing visibility and automating threat response across multiple attack vectors, including email, endpoints, networks, cloud, and servers. The latest wave of innovation in XDR is powered by sophisticated AI and machine learning models that identify anomalies and adapt to evolving threat patterns in real time. These tools allow MSSPs and in-house security teams to move beyond traditional rule-based detections and enable predictive threat hunting, reducing the dwell time of undetected attacks. Real-world deployments highlight the way businesses are adopting XDR to modernize their security posture. For instance, Trend Micro's Vision One XDR platform and Microsoft Defender XDR are being leveraged by large enterprises to unify security telemetry, enrich alerts with contextual intelligence, and orchestrate faster, automated incident response. These platforms integrate seamlessly with SIEM and SOAR systems, incorporating User and Entity Behavior Analytics (UEBA) to detect insider threats and credential-based attacks critical for industries like finance, healthcare, and manufacturing.

Cloud-native XDR platforms are rising in popularity as they offer the scalability and flexibility required by globally distributed organizations. CrowdStrike and Palo Alto Networks are offering fully cloud-native XDR solutions that provide holistic threat visibility and automated playbooks across cloud workloads. This evolution ensures that XDR is no longer just an add-on but a core pillar of modern security architecture, delivering unified, automated, and intelligent threat detection and response at scale.

3.11 PATENT ANALYSIS

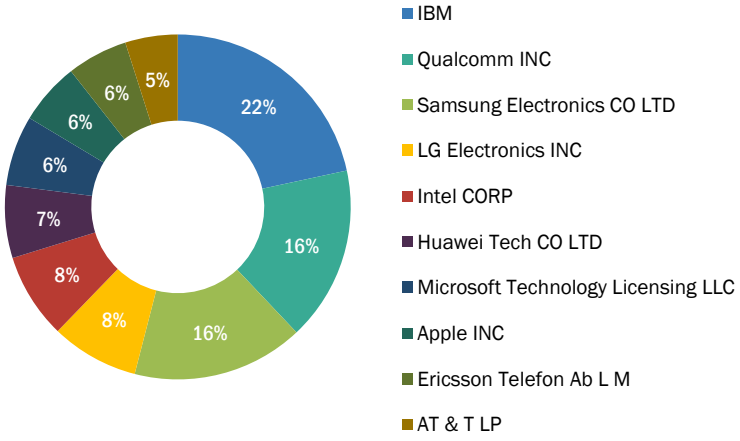
The analysis of patents provides valuable insights into patent filings, business interests, and patenting activities on a year-to-year and country-specific basis. This method serves as a means to comprehend the information encapsulated within patents. This analysis reveals valuable insights into innovation trends, intellectual property strategies, and the shifting focus of technology vendors. Year-over-year patent filings suggest increased interest in developing advanced capabilities such as AI-driven threat detection, cloud-native security orchestration, and zero-trust architectures. Managed security service providers are focusing

heavily on technologies that enhance automation, scalability, and real-time monitoring. This includes the development of proprietary security orchestration, automation, and response (SOAR) platforms, next-generation firewall integration, and intelligent SIEM (Security Information and Event Management) systems. These innovations are often protected through patent filings that safeguard intellectual property and create competitive differentiation.

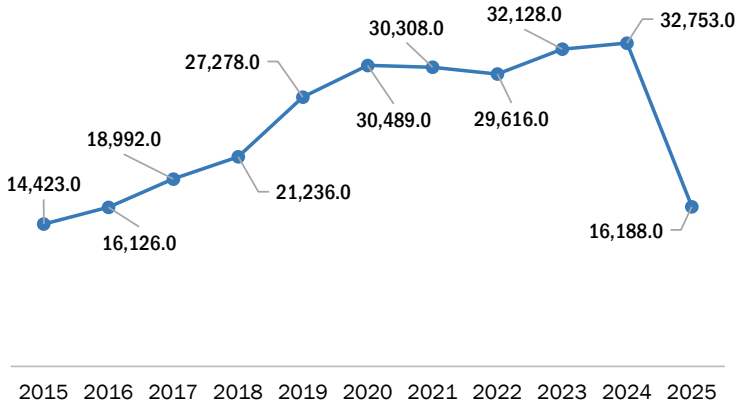
This section explores the prevailing industry relationships among stakeholders, including research and development (R&D) organizations, regulatory bodies, government agencies, managed security service providers, cloud infrastructure vendors, and cybersecurity technology developers. It assesses product innovations and applications by providing an overview of patents. Over the last decade, the MSS market has seen significant momentum in patent filings associated with secure network access, behavioral analytics, and blockchain-based audit mechanisms.

FIGURE 14 NUMBER OF PATENTS GRANTED FOR MANAGED SECURITY SERVICES MARKET, 2015–2025

TOP 10 COMPANIES WITH HIGHEST NUMBER OF PATENT APPLICATIONS IN LAST 10 YEARS



PATENTS PUBLISHED IN OVER A YEAR FOR 10 YEARS

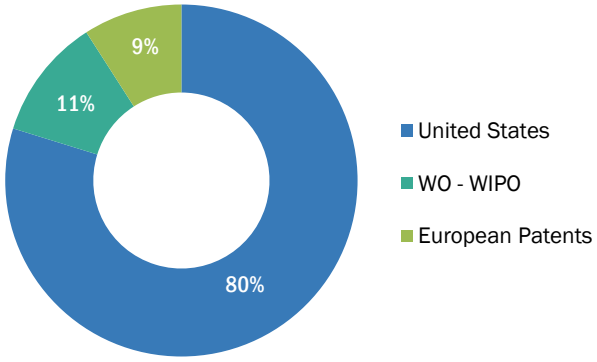


TOP 20 PATENT OWNERS IN THE LAST 10 YEARS

Company Name	No. of Patents
IBM	22,116
Qualcomm INC	16,721
Samsung Electronics CO LTD	16,428
LG Electronics INC	8,394
Intel CORP	8,184
Huawei Tech CO LTD	6,982
Microsoft Technology Licensing LLC	6,725
Apple INC	5,933
Ericsson Telefon Ab L M	5,814
At & T Ip I LP	5,023
Cisco Tech INC	4,594
Oracle Int CORP	4,046
Google LLC	3,880
Dell Products LP	3,449
Capital One Services LLC	3,446
Snap INC	3,128
Amazon Tech INC	3,110
Interdigital Patent Holdings INC	2,928
VmWare INC	2,435
Salesforce Com INC	2,412

Source: Lens.org and MarketsandMarkets Analysis

FIGURE 15 REGIONAL ANALYSIS OF PATENTS GRANTED FOR MANAGED SECURITY SERVICES MARKET



Note: Patents have been considered from January 2015 to July 3, 2025.

Source: Lens.org and MarketsandMarkets Analysis

TABLE 9 LIST OF FEW PATENTS IN MANAGED SECURITY SERVICES, 2024–2025

APPLICANT	PUBLICATION NUMBER	YEAR	DESCRIPTION
Cupp Computing As	US 2025/ 0061200 A1	Feb 2025	This invention presents a system and method that supports the principles of MSS by enabling a mobile security system to autonomously manage security functions even when a device is in power management mode. By detecting wake events and issuing wake signals, the system ensures that critical security tasks such as malware scanning, unauthorized data detection, and security application updates are performed without requiring user intervention. This approach mirrors MSS objectives by maintaining continuous protection, real-time threat monitoring, and system integrity during low-power or idle states, effectively eliminating security gaps typically associated with reduced device activity.
Acronis Int GmbH	US 1215 5627 B2	Nov 2024	This invention enhances firewall policy control within MSS by enabling centralized management and synchronization of endpoint firewall policies, including dynamic isolation capabilities. A centralized firewall management service coordinates with local agents installed on managed endpoints to deploy, modify, or revoke firewall policies, ensuring consistent enforcement across the network. The system supports conflict resolution between local and central policies, prioritizing centrally defined rules unless the conflict originates from the central service itself. This architecture allows MSSPs to maintain secure, real-time policy control, including isolating compromised endpoints, while balancing centralized authority with endpoint autonomy.
Amazon Tech Inc	US 1211 1940 B1	Oct 2024	This invention enables the enforcement of security policies for operating system resource access through an external policy management service, supporting MSS. By intercepting system calls via a kernel-mode component and delegating authorization decisions to a centrally managed policy service, the system ensures consistent, scalable, and dynamic access control aligned with enterprise security requirements. This externalized policy enforcement, with optional caching for efficiency, reflects MSS principles by centralizing policy management, reducing endpoint complexity, and allowing managed service providers to maintain tighter control over system-level security across customer environments, including those running mainframe workloads.
Honeywell	US 1213	Oct	This invention presents a system and method for providing connected access

International Inc	0905 B2	2024	control through a dual-platform architecture that supports dynamic and centralized management of access credentials and security events within managed services. The first access control platform handles real-time events such as hardware triggers, access requests, and management actions by validating them against stored permissions and event data. The second platform oversees higher-level updates, including modifying access permissions and managing security device records. This layered approach enhances operational control, ensures accurate access enforcement, and supports scalable, remotely managed security infrastructure in environments requiring continuous monitoring and credential governance.
Dropzone Ai Inc	US 1210 5746 B1	Oct 2024	This invention provides intelligent monitoring of security environments in support of MSS through dynamic querying and contextual analysis. A survey engine builds a subject index from various data sources, and a query engine uses client questions to retrieve and rank relevant security information using trained models. This approach allows MSS providers to deliver accurate, data-driven insights and responses, enhancing threat detection, investigation, and overall situational awareness.
Palantir Technologies Inc	US 1208 1523 B1	Sept 2024	This invention enables dynamic and automated firewall rule management between services by leveraging real-time discovery data and API dependencies, aligning with the goals of MSS. By analyzing a discovery graph of service interactions, the system identifies valid communication paths and generates corresponding firewall rules. This reduces manual configuration, improves policy accuracy, and strengthens security across complex, distributed, or microservice-based environments. It allows MSS providers to deliver scalable, context-aware access control while minimizing the risk of misconfigurations and unauthorized service communication.
Servicenow Inc	US 1206 7127 B2	Aug 2024	This invention allows automated detection, assessment, and communication of software vulnerabilities across managed networks, supporting the goals of MSS. By analyzing configuration data from computing devices and installed applications, the system identifies vulnerable software, calculates a threat score based on severity and deployment scale, and delivers tailored insights to relevant stakeholders. This approach enhances MSS by providing centralized visibility, prioritized risk evaluation, and actionable intelligence empowering service providers to proactively mitigate risks and support informed security decisions across distributed environments.
Emc IP Holding Co LLC	US 1194 1155 B2	Mar 2024	This invention represents centralized and automated secure data management across networked computing environments. A security management system classifies incoming data by sensitivity and applies appropriate encryption levels before sending it to a cloud system for secure storage or analytics. This approach enforces data protection policies, ensures compliance with security standards, and delivers scalable, policy-driven encryption, enhancing data governance and reducing risk in distributed and cloud-integrated infrastructures.
Mastercard International Inc	US 1190 9721 B2	Feb 2024	This invention presents a system that enables managed firewall functionality within MSS by automating the creation and deployment of VM-specific firewall rules based on group-level policies. A firewall configuration server receives group-based rules and VM membership data, parses this information, and generates tailored firewall rules for each VM. These rules are then applied to control network traffic, allowing MSS providers to deliver scalable, consistent, and centralized security across dynamic virtual environments.

Source: Lens. Org—Patent and Scholarly Search and MarketsandMarkets Analysis

3.12 REGULATORY LANDSCAPE

3.12.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

This section includes a region-wise list of key regulatory bodies, government agencies, industry associations, and non-profit organizations relevant to the MSS market.

TABLE 10 NORTH AMERICA: REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
US	National Institute of Standards and Technology (NIST)-Cybersecurity	Government Agency	Develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of the broader public
US	Cybersecurity and Infrastructure Security Agency (CISA)	Government Agency	Leads national efforts to improve cybersecurity infrastructure, including MSS adoption
US	Federal Trade Commission (FTC)	Regulatory Authority	Enforces data protection rules and regulates MSS practices in consumer-focused industries
US	Center for Internet Security (CIS)	Non-profit Organization	Provides benchmarks and best practices for MSS providers and IT security operations
Canada	Canadian Centre for Cyber Security (CCCS)	Government Agency	Offers national guidance on cybersecurity services, risk frameworks, and MSS integration
Canada	Public Safety Canada	Government Regulatory	Promotes the safety and security of Canadians with a prime focus on national security, border strategies, countering crime, and emergency management

Source: Secondary Research and MarketsandMarkets Analysis

TABLE 11 EUROPE: REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
EU	European Union Agency for Cybersecurity (ENISA)	Government Agency	Develops cybersecurity frameworks, policies, and supports MSS providers across the EU
EU	European Data Protection Board (EDPB)	Regulatory Body	Ensures consistent GDPR enforcement and impacts MSS compliance mandates
Germany	Federal Office for Information Security (BSI)	Government Agency	Sets IT security standards and certifies MSS providers in Germany
UK	National Cyber Security Centre (NCSC UK)	Government Agency	Offers best practices and incident response guidance for MSSPs operating in the UK

France	National Cybersecurity Agency of France (ANSSI)	Government Agency	Regulates national cybersecurity strategy, certifies MSS vendors in critical sectors
EU	Cloud Security Alliance (CSA) – Europe Chapter	Non-Profit Organization	Promotes cloud and MSS security standards through education and certifications
EU Member States	GDPR	Government Regulatory	Toughest privacy and security law in the world Aims to give individuals control over their data and simplify the regulatory environment for international business by unifying the regulations in the EU

Source: Secondary Research and MarketsandMarkets Analysis

TABLE 12 ASIA PACIFIC: REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
India	Indian Computer Emergency Response Team (CERT-In)	Government Agency	Coordinates MSS incident response and issues security advisories for critical sectors
Singapore	Cyber Security Agency of Singapore (CSA)	Government Agency	Develops national cybersecurity policies and regulates MSS operations and standards
Australia	Australian Cyber Security Centre (ACSC)	Government Agency	Leads national efforts on MSS best practices, threat alerts, and cyber readiness
Japan	National center of Incident readiness and Strategy for Cybersecurity (NISC)	Government Agency	Oversees Japan's MSS policies, critical infrastructure protection, and coordination
China	Cyberspace Administration of China (CAC)	Regulatory Body	Regulates MSS-related data protection and network security under national law
Thailand	National Cyber Security Agency (NCSA) - Thailand	Government Agency	Coordinates and implements national cybersecurity policies, strategies, and initiatives
Asia-Pacific Region	Asia Pacific Computer Emergency Response Team (APCERT)	Non-Profit Organization	Fosters cooperation among MSS providers and national CERTs across the Asia Pacific
China	China's Data Security Law and Cybersecurity Law	Government Regulatory	Operator of a critical information infrastructure stores important data collected and generated domestically within China
Australia	Australian National Security Law	Government Regulatory	Counter-terrorism legislation: a critical element of Australia's national security framework

Source: Secondary Research and MarketsandMarkets Analysis

TABLE 13 MIDDLE EAST & AFRICA: REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
UAE	UAE Cybersecurity Council	Government Agency	Oversees national cybersecurity strategy and MSS regulations across sectors
Saudi Arabia	National Cybersecurity Authority (NCA)	Government Agency	Develops MSS frameworks, compliance policies, and risk mitigation programs
South Africa	South African Cybersecurity Hub (under Department of Communications and Digital Technologies)	Government Agency	Coordinates national MSS efforts, incident response, and public-private collaboration
Qatar	National Cyber Security Agency- Qatar	Government Agency	Establishes MSS policies, oversees cybersecurity compliance, and threat defense
Ethiopia	African Union Cyber Security Expert Group	Regional Coordination Body	Promotes harmonized MSS policy frameworks and CERT collaboration across African states

Source: Secondary Research and MarketsandMarkets Analysis

TABLE 14 LATIN AMERICA: REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
Brazil	Brazilian National Data Protection Authority (ANPD)	Regulatory Body	Enforces Brazil's LGPD law, shaping MSS data governance and breach notification rules
Mexico	National Cybersecurity Coordination (CNCS)- Mexico	Government Agency	Oversees national MSS coordination and cyber defense policy
Chile	Cybersecurity Unit – Ministry of Interior and Public Security	Government Agency	Drives MSS strategies, risk management, and incident response
Argentina	Directorate of Cybersecurity and Critical Infrastructure Protection (DCIPIC)	Government Agency	Develops MSS frameworks and ensures infrastructure resilience
Colombia	Colombian Cyber Emergency Response Group (colCERT)	Government Agency	Coordinates MSS-related threat intelligence, alerts, and incident response
Uruguay	National Directorate of Information and Communication Technologies (AGESIC)- Cybersecurity	Government Agency	Oversees MSS policies, cybersecurity governance, and public-private MSS initiatives

Source: Secondary Research and MarketsandMarkets Analysis

3.12.2 KEY REGULATIONS

3.12.2.1 Payment Card Industry Data Security Standard (PCI–DSS)

PCI-DSS compliance, jointly developed by major payment brands such as American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa International, outlines 12 requirements aimed at enhancing the security of payment account data. These requirements encompass the establishment of policies, deployment of tools, and implementation of controls to safeguard cardholder data. The standard mandates that merchants and Member Service Providers (MSPs) handling cardholder data establish and maintain secure IT networks, protect such data, conduct vulnerability management, enforce robust access controls, and regularly monitor and test networks.

The primary goal of PCI DSS is to prevent data breaches. To achieve this, businesses must use security software to protect against threats, control physical access to sensitive information, and thoroughly test their network security to minimize risks for card companies and their customers. Companies are encouraged to adopt top-tier digital forensic solutions, which can help them recover lost data in the event of a potential breach. These solutions also facilitate investigations into data storage locations, including local and remote storage areas, eCommerce websites, and payment gateways. By following these guidelines and implementing these solutions, businesses can maintain PCI DSS compliance and reduce the risk of cyber threats.

3.12.2.2 General Data Protection Regulation (GDPR)

The GDPR is a regulation that the European Parliament has imposed. It requires enterprises to adopt strict cybersecurity solutions to protect enterprise data. The Council of the European Union (EU) and the European Commission enforce GDPR to ensure the protection and privacy of EU citizens, even if data is exported outside the EU. GDPR unifies all major regulations that fall within the EU, and it has replaced the Data Protection Directive that was commissioned in 1995. It was adopted on April 27, 2016, and became effective on May 25, 2018.

Noncompliance with the GDPR regulation may result in severe penalties, which could be up to 4% of the annual enterprise revenue. Some significant GDPR requirements include data breach notifications, secure data transfer, anonymization of customer data, and data processing with client consent. GDPR also mandates that enterprises conduct thorough post-breach digital investigations to recover lost data and to detect any indicators of doubt that may be a result of internal or external activities. Digital forensic solutions assist with detection, recovery, analysis, and reporting, thereby helping enterprises recover from breaches and ensure compliance with GDPR.

3.12.2.3 California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act was signed into law in 2018 and grants consumers greater control over the personal information that businesses collect about them. This law creates new privacy rights for Californians and imposes new data protection obligations on companies. California consumers have privacy rights, including the right to know, delete, opt out, and be free from discrimination. The CCPA applies to for-profit businesses that do business in California and have a gross annual revenue of over USD 25 million, buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices, or derive 50% or more of their annual revenue from selling California residents' personal information.

The CCPA regulations provide guidance for businesses to comply with the CCPA. These regulations help businesses inform consumers of their rights under the CCPA, handle consumer requests, verify the identity of consumers making requests, and apply the law to minors.

3.12.2.4 Gramm-Leach-Bliley Act of 1999 (GLBA)

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is a federal law in the United States that regulates how financial institutions handle individuals' private information. It includes provisions to protect the personal financial data of consumers held by banks, securities firms, and insurance companies. The enforcement of GLBA is overseen by the Federal Trade Commission (FTC), which requires these financial institutions to establish, implement, and maintain information security programs to ensure the privacy and security of customer data. To comply with GLBA guidelines, financial institutions rely on cybersecurity solutions provided by well-known security vendors. These solutions help institutions conduct risk assessments and implement security monitoring strategies.

Digital forensic solutions and services also play a crucial role in ensuring the security of customer data, especially for entities such as mortgage lenders, real estate firms, loan brokers, investment consulting firms, debt collection firms, and tax consulting firms. The adoption of digital forensic solutions and services has become necessary due to the increasing instances of financial fraud and the use of sophisticated cyber-attack tools. Financial firms understand the importance of these measures in safeguarding customer data and maintaining the integrity of their operations in an environment marked by evolving cybersecurity threats and risks.

3.12.2.5 Personal Information Protection and Electronic Documents Act (PIPEDA)

As per the Personal Information Protection and Electronic Documents Act (PIPEDA), organizations must comply with the law while handling personal data. Additionally, the Act promotes electronic alternatives for dealing with government entities. Part 2 of the Act, known as “Electronic Documents,” aims to establish equal treatment between electronic and paper mediums. This allows for the electronic adaptation of federal laws, which previously required paper documentation. Although this part does not mandate changes, it permits authorities to create regulations for electronic compliance.

It also defines secure electronic signatures, which must be unique, under user control, and ensure identification and document integrity. Part 3 amends the Canada Evidence Act, making electronic documents admissible in court and recognizing secure electronic signatures. Part 4 grants electronic notices the same legal standing as paper versions, while Part 5 authorizes electronic publication of Canadian statutes and regulations, giving them official status.

3.12.2.6 Federal Information Security Management Act (FISMA)

In 2002, the US government established the FISMA law to enhance computer and network security for federal entities and affiliated parties, including government contractors. The law requires the implementation of information security controls and regular audits. The National Institute of Standards and Technology (NIST) is responsible for developing and managing technical standards for compliance. This involves categorizing information to be protected, selecting minimum controls, and refining them through risk assessment. The controls are documented in a system security plan, implemented in appropriate systems, and assessed for effectiveness.

Agencies must determine risks to their mission or business case and authorize information systems for processing while continuously monitoring security controls. Annual reviews of cybersecurity programs help minimize business risks. Cyberattacks on the federal government have increased due to regional and national rivalries, cybercriminal and terrorist activities, and other factors. To secure the government, solutions such as Security Information and Event Management (SIEM), network access control, data loss prevention, web application firewall, secure web gateway, digital forensics, and incident response are necessary.

3.12.2.7 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA compliance protects personal health information at the federal level, giving patients the right to safeguard their own PHI and ensuring data privacy and security for medical information. As the healthcare industry shifts toward electronic records accessible via web and mobile applications, hackers often target this sensitive patient data. To comply with HIPAA guidelines, web and mobile applications transmitting, storing, or sharing data related to doctors, patients, or other health-related information must adhere to policies and procedures to safeguard healthcare records. Non-compliance with these policies and procedures is the most common cause of HIPAA violations.

Organizations handling PHI must implement and adhere to necessary physical, process, and network security measures. HIPAA mandates that healthcare enterprises and organizations rely heavily on digital forensics to track and document suspect indicators that may have played a role in data breach events. HIPAA emphasizes adopting digital forensics solutions proactively rather than reacting after an incident. Additionally, HIPAA emphasizes the adoption of digital forensic solutions that aid data preservation, restoration of electronic protected health information (EPHI), user activity monitoring, and reporting.

3.12.2.8 Sarbanes-Oxley Act (SOX)

In 2022, the US Congress passed the SOX legislation to safeguard shareholders and the public from fraudulent practices and accounting errors committed by enterprises. This law also aims to enhance the precision of corporate disclosures. SOX was designed with the primary objective of promoting transparency in corporate governance and financial reporting by establishing a system of internal checks and balances. Failure to comply with SOX regulations may result in penalties such as fines and removal from public stock exchanges. To meet SOX compliance, cybersecurity vendors offer solutions for risk assessment, intrusion detection, network forensics, and security monitoring based on industry best practices.

Nowadays, attackers usually target financial transaction applications, and any security loophole in such applications may jeopardize data integrity. Therefore, organizations must ensure that these applications undergo thorough vulnerability testing to guarantee data security. Public companies must feel financially secure in the event of a breach. This law also emphasizes the importance of C-level executives developing robust digital forensic strategies and adopting best-in-class digital forensic solutions to prevent digital fraud and breaches. In case of a cyber-attack, digital forensics can assist in data recovery and analysis from every affected storage device, network, cloud environment, or virtual environment. To comply with SOX, public companies should pay close attention to any doubts that may impact the smooth functioning of their enterprises.

3.12.2.9 International Organization for Standardization (ISO) – Standard 27001

ISO 27001 compliance, established by the International Organization for Standardization (ISO), offers a risk-based framework for developing, implementing, and managing an Information Security Management System (ISMS). This involves creating policies and procedures, defining the ISMS's security policy and scope, conducting risk assessments, managing identified risks, selecting control objectives and measures, and preparing a statement of applicability. ISO 27001 guidelines encompass various areas, including access control, audit, incident response, system, and information integrity. Of the 150 controls mandated by ISO 27001 compliance, the 11 major controls include security policy, information security organization, asset management, human resource security, physical and environmental security, communications and operations management, access control, information systems acquisition, development, and maintenance, information security incident management, business continuity management, and compliance.

3.13 IMPACT OF 2025 US TARIFF – MANAGED SECURITY SERVICES MARKET

3.13.1 INTRODUCTION

The reimplementation of U.S. reciprocal tariffs in July 2025, following the expiry of the 90-day pause on July 9, has significantly disrupted the global landscape for MSS. These tariffs, ranging from 10% to over 50%, are targeted at critical cybersecurity hardware and services, including routers, firewalls, IDS/IPS systems, threat detection appliances, and encryption hardware—many of which are central to MSS operations. The policy has impacted MSSPs with hardware-centric delivery models, such as those providing on-premises SOC infrastructure or bundled appliance-based MSS contracts. China's 125% retaliatory tariffs on U.S.-origin cybersecurity components, combined with Europe's proposed 25% duties on U.S. cybersecurity services, have further intensified pressures on MSS providers, increasing costs and disrupting cross-border managed service delivery. As a result, MSSPs globally are now shifting toward cloud-based SOC-as-a-Service (SOCaaS) models, diversifying hardware vendors geographically, and revisiting long-term client contracts to hedge against future volatility.

Key Implications include:

- Tariffs have significantly raised costs for MSSPs relying on US-made cybersecurity hardware, increasing the total cost of ownership (TCO) for clients.
- Tariff-related restrictions are causing delays in hardware sourcing and MSS deployments due to rerouted logistics and vendor shifts.
- MSSPs are accelerating the adoption of cloud-native SOCaaS and MXDR solutions to reduce hardware dependency and deployment risks.
- Providers are diversifying their supply chains, sourcing hardware from non-tariffed regions to reduce exposure to geopolitical volatility.
- MSSPs are renegotiating long-term contracts to include tariff clauses and flexible pricing, aiming to safeguard margins and service continuity.

3.13.2 KEY TARIFF RATES

TABLE 15 KEY TARIFF RATES

SR.NO	COUNTRY	KEY MSS-RELATED COMPONENTS AFFECTED	ESTIMATED TARIFF (%)	EFFECTIVE DATE	MSS IMPACT LEVEL	REMARKS/CONFIDENCE LEVEL
1	China	Firewalls, IDS appliances, NDR modules	~30%	July 10, 2025	High	Tariffs widely reported; MSS highly hardware-dependent; confirmed via Maersk & policy trackers
2	Japan	GPUs, advanced analytics hardware	24%	July 10, 2025	Medium-High	Matches general electronics tariffs; impacts high-end AI/ML tools
3	South Korea	SIEM servers, monitoring sensors	25%	July 10, 2025	Medium	Confirmed 25% reciprocal duty; MSS vendors may face cost pressure
4	Taiwan	Log collectors, edge boxes	32%	July 10, 2025	High	Higher tariffs aligned with sensitive electronics category

5	Mexico	Cable assemblies, low-cost SOC gear	25%	July 10, 2025	Medium	Confirmed under the US general electronics duty list
6	Germany	Encryption modules, identity appliances	20%	July 10, 2025	Medium-Low	Not a direct target, but faces reciprocal measures on sensitive MSS inputs
7	India	Software exports, workstations (proposed)	52% (proposed)	July 10, 2025	Risk Escalation Zone	No formal implementation yet; policy discussions ongoing. Potential MSS software delivery impact

**Tariff rates listed are effective as of July 10, 2025, and are subject to change based on ongoing trade negotiations and regulatory updates.*

Source: WITS, World Bank, White House Press Release, and Desk Research

The 2025 US tariffs have reshaped the global MSS landscape by driving up costs on Chinese-origin cybersecurity infrastructure, including firewalls, IDS/IPS appliances, and secure routers. The 25% duty on critical hardware and embedded systems has raised MSS operational expenses by an estimated 12–18%, leading to slower deployments, particularly in finance, healthcare, and critical infrastructure. North American and European MSS providers have been most impacted due to their reliance on Chinese hardware imports. In response, major players such as IBM Security and Orange Cyberdefense are fast-tracking the adoption of AI-powered threat detection, SaaS-based SIEM, and virtual SOC models to reduce hardware exposure. Enterprises are also diversifying sourcing strategies, shifting toward tariff-exempt suppliers such as those in South Korea and expanding internal cybersecurity capabilities to ensure service continuity and regulatory compliance amid persistent cost pressures.

3.13.3 PRICE IMPACT ANALYSIS

The July 2025 tariff enforcement has triggered a notable rise in MSS delivery costs, with hardware prices increasing by 7% to 28% depending on device type and origin. MSSPs with appliance-heavy models—particularly those bundling SIEM, IDS, and log monitoring are most affected. As a result, providers are shifting to cloud-native SOCaaS/XDR models, adopting hardware leasing strategies, and renegotiating long-term contracts to include price escalation clauses, aiming to manage the financial impact and maintain service continuity.

Strategic responses adopted by MSS providers:

- Cloud-first MSS offerings: Shift to SOCaaS/XDR models with reduced dependency on physical devices.
- Inventory pre-purchase: MSSPs are stockpiling critical hardware prior to future tariff rounds.
- Geographic vendor diversification: Shifting sourcing from China, Japan, and Korea to Southeast Asia, LATAM, and Eastern Europe.
- Service bundling and modular pricing: Providers are unbundling hardware and software layers to isolate tariff-driven cost increases.
- Strategic shift & emerging trends:
- Cloud-native Security Operations: MSS providers are rapidly shifting to cloud-hosted SOCs to minimize reliance on hardware subject to tariffs, enhancing flexibility and scalability.
- Globalization of SOC Infrastructure: Vendors are establishing SOC nodes in low-tariff countries like Vietnam, Poland, and the UAE to optimize costs and maintain global service delivery.

- Sovereign MSS Architectures: Governments in Asia and the Middle East are increasingly mandating regionally hosted MSS platforms to ensure data control and reduce foreign dependency.
- Open-source Security Frameworks: Providers are adopting open-source tools for detection, analytics, and orchestration to lower costs and avoid proprietary software constraints.

TABLE 16 EXPECTED CHANGE IN PRICES AND LIKELY IMPACT ON END-USE MARKET DUE TO TARIFF IMPACT

END-USE CATEGORY	TARGET PRODUCT (PRICE CHANGE)	END-USE PRODUCT (PRICE CHANGE)	KEY PRODUCTS (PRICE INCREASES)	KEY PLAYERS IMPACTED
BFSI	Next-Gen Firewalls, SIEM Licenses (+23%)	Threat Detection Tools (+20%)	Behavioral Analytics, Risk Engines (+22%)	Palo Alto, IBM, Fortinet, Infosys
Healthcare	Secure Endpoints, HIPAA-compliant VPNs (+21%)	SOC-as-a-Service (+19%)	Endpoint Detection & Response, MDR Tools (+20%)	Atos, TCS, Sophos, Cisco
Government	Encrypted Routers, Classified Firewalls (+25%)	Managed SOC Terminals (+21%)	Document Protection Tools, Zero Trust Frameworks (+24%)	NEC, DXC, Verizon, BAE Systems
Retail	Network Switches, Secure POS Routers (+20%)	Cloud SIEM, Retail Endpoint Monitoring (+19%)	Threat Intelligence Feeds, SIEM Dashboards (+20%)	Trustwave, SonicWall
IT & ITeS	Data Center Servers, IDS/IPS Systems (+24%)	Hybrid Cloud SOC (+22%)	AI Threat Analytics, Cloud Firewalls (+23%)	Accenture, IBM Security, Kyndryl

Source: WITS, World Bank, White House Press Release, and Desk Research

The reimposition of tariffs on Chinese-made network security hardware and threat detection systems has significantly elevated costs across firewalls, IDS/IPS appliances, secure routers, and SOC-integrated modules. Core components such as traffic inspection units, AI-enabled sensors, encrypted gateways, and endpoint detection tools have experienced price increases ranging from 18% to 25%. These cost escalations are straining MSS procurement for finance, healthcare, public services, and education sectors, particularly among regional providers and institutions facing tight IT security budgets or compliance mandates requiring 24/7 managed defense capabilities.

3.13.4 IMPACT ON COUNTRY/REGION

3.13.4.1 North America

The North American MSS market in 2025 is undergoing a strategic transformation due to significant tariff shocks on cybersecurity infrastructure, affecting hardware-dependent service models. While the US faces direct tariff pressures, Canada and Mexico are experiencing indirect cost escalation due to regional supply chain exposure. Across the region, MSS providers are shifting toward virtualized SOC models, cloud-native threat monitoring, and AI-based automation to reduce reliance on high-cost imported equipment. Public and private sector clients are increasingly prioritizing flexible, SLA-backed service contracts to maintain resilience amid fluctuating costs.

US

The US-based MSSPs are facing steep cost increases driven by tariffs on imported cybersecurity components such as firewalls, intrusion detection systems, and telemetry hardware. Appliance-heavy MSS deployments are particularly impacted, pushing MSSPs toward domestic hardware sourcing and cloud-first security operations. IBM and AT&T are expanding leasing models and promoting virtual SOCs to reduce capital expenditure. Public-sector clients are restructuring contracts with fixed-term SLAs to offset price volatility, while delays in imported hardware shipments have extended SOC deployment cycles by up to 45 days. MSSPs are also ramping up investments in AI-driven detection and SaaS-based SIEM tools to future-proof operations.

Canada

Although partially insulated under USMCA, Canadian MSSPs are still facing indirect cost pressures due to reliance on US-assembled devices containing tariffed Chinese components. These include secure gateways, network analyzers, and traffic encryption hardware, with observed price hikes of 12–16%. To mitigate this, Canadian providers are forming partnerships with local hardware integrators and expanding their focus on cloud-native threat monitoring services. As the market shifts away from hardware-centric deployments, MSSPs are accelerating the adoption of open-source tools and modular SOC solutions to maintain service delivery without passing excessive costs onto clients.

Mexico

Mexican MSS providers are experiencing hardware procurement delays and increased costs due to 25% import duties on Chinese-origin cybersecurity products not covered under USMCA. These include DLP systems, endpoint sensors, and high-throughput routers, especially critical for large-scale enterprise and public-sector deployments. As a result, providers are facing extended deployment cycles, rising total cost of ownership, and operational constraints in key industries such as logistics, manufacturing, and finance. To adapt, MSSPs are pursuing collaborative programs with U.S. vendors for local device configuration and support, while also investing in software-defined security models and regional sourcing alternatives in Latin America and Southeast Asia.

Market Challenges:

- High tariffs on imported security hardware raise MSS delivery costs by 20–28%.
- Delayed deployment cycles and longer procurement timelines affect SLA compliance.
- Federal clients require cost-predictable, resilient MSS strategies amid budget constraints.

Mitigation Measures:

To mitigate rising tariff costs, MSSPs are increasingly adopting domestic manufacturing strategies and transitioning to virtualized SOC models to reduce reliance on imported hardware. Public-sector contracts are being restructured with SLA-based frameworks to ensure service continuity and cost predictability. Simultaneously, providers are accelerating investments in AI-driven threat detection, SaaS-based SIEM platforms, and hybrid deployment models that minimize hardware dependency and enhance operational resilience.

3.13.4.2 Europe

Reciprocal tariffs on US-origin MSS tools and global electronics inflation have raised core MSS deployment costs in Europe by 14–21%. EU-based MSSPs such as Orange Cyberdefense and Capgemini are shifting sourcing to local and Asian vendors, adopting open integration frameworks, and prioritizing cloud-hosted SOC models to bypass physical import constraints. These changes come amid rising demand for flexible, standards-compliant security solutions aligned with NIS2 and GDPR directives, particularly in finance, healthcare, and public administration sectors.

Germany

Germany, a leader in industrial cybersecurity, is experiencing hardware-related MSS cost hikes of up to 23%, affecting SIEM systems, secure endpoints, and segmentation platforms. Federal and regional cybersecurity initiatives are being delayed as Lander governments await additional EU Digital Europe Programme co-financing. Providers are transitioning to open-source security stacks and hybrid SOC architectures to mitigate CapEx exposure.

France

France's centrally coordinated procurement system has softened some of the price impact, yet MSSPs still face 16–19% cost increases on AI-powered analytics and encrypted access systems. Public-sector MSS efforts are now focused on critical infrastructure protection and regulatory compliance. Unified threat detection solutions that meet NIS2 standards are seeing growing traction among enterprise and government clients.

UK

Post-Brexit, UK MSSPs are grappling with compounded tariff exposure and funding limitations. The 10% US electronics tariff and lack of EU cybersecurity financing are inflating costs of cross-border SOC systems, VPN hardware, and threat intelligence modules. Rollout delays are particularly acute in national monitoring projects and public-sector hybrid cloud deployments. To adapt, the UK is negotiating bilateral cybersecurity tech exchanges and boosting domestic MSS R&D through targeted tax incentives.

Market Challenges:

- Uneven mitigation strategies across EU states hamper coordinated MSS responses
- Regional funding disparities are delaying security upgrades and cloud transitions
- Supply shortages for GDPR- and NIS2-compliant infrastructure
- Divergent compliance requirements across EU, EFTA, and UK jurisdictions

Mitigation Measures:

Mitigation efforts across Europe are being strengthened through expanded investment via the European Cybersecurity Competence Centre (ECCC), which is channeling resources toward next-generation MSS capabilities. The EU is also deploying Digital Decade funds to support joint MSS innovation initiatives and collaborative procurement platforms that reduce duplication and improve cost efficiency. In parallel, regional cloud-based SOC infrastructures and vendor-neutral integration frameworks are being developed to lower reliance on tariffed hardware and promote interoperability. In the UK, which lacks access to EU cybersecurity funding post-Brexit, the government is incentivizing local MSS innovation through tax credits, targeted R&D grants, and bilateral technology exchange agreements with trusted international partners.

3.13.4.3 Asia Pacific

Asia Pacific's MSS market is navigating dual pressures, rising equipment costs due to U.S.-China tariff tensions, and growing demand from Western clients seeking low-tariff service hubs. Overall, MSS infrastructure costs have risen up to 24% for intrusion detection systems, SIEM appliances, and encryption hardware. In response, many APAC nations are accelerating local manufacturing and embracing cloud-hosted SOCs. Cost-conscious industries, such as BFSI, telecom, and public sector programs, are either deferring upgrades or shifting to locally integrated and virtualized MSS platforms. Governments across the region are launching support programs for domestic cybersecurity infrastructure to reduce reliance on tariffed imports and enhance self-sufficiency.

China

China's MSS market is facing strong headwinds from the 125% US tariff on key components, such as security chipsets and advanced detection modules. Export demand has weakened, and domestic projects are burdened by cost inflation and limited access to Western technology. In response, Chinese vendors are promoting end-to-end MSS solutions built entirely on local infrastructure. However, these platforms are still maturing in interoperability and advanced threat coverage, raising questions about their global competitiveness.

India

India's MSS sector, one of the fastest-growing globally, is contending with 15–20% increases in the cost of imported threat detection and SIEM tools, particularly those reliant on US-based AI/ML engines. To mitigate this, the government is incentivizing domestic MSS production through Production Linked Incentive (PLI) schemes and Digital India-aligned grants. Indigenous MSS pilots built on local cloud and telemetry infrastructure are underway in urban hubs, positioning India as a potential alternative hub for MSS innovation and delivery.

Japan

Japan is experiencing 16–18% MSS infrastructure cost increases, primarily impacting secure telemetry devices and high-assurance onboarding systems vital to sectors like banking and immigration. These pressures stem from supply chain disruptions linked to U.S.-China tensions. In response, Japan is boosting domestic R&D, enhancing procurement from Taiwan and ASEAN partners, and encouraging cybersecurity collaborations to maintain SOC operational integrity and protect critical systems from pricing shocks.

Market Challenges:

- High dependency on imported MSS hardware amid global tariff hikes
- Delays in national cybersecurity upgrades and public-sector SOC rollouts
- Limited domestic production capacity for advanced cybersecurity gear
- Tariff-driven cost surges affecting scalability across essential sectors

Mitigation Measures:

Asia Pacific countries are expanding domestic MSS production via tax credits, grants, and vendor incubation. India's "Make in India" strategy is being extended to mobile SOCs and endpoint detection tools. Japan is fostering joint ventures and diversifying sourcing away from China. Across APAC, Vietnam, Malaysia, and South Korea are emerging as key low-tariff alternatives for MSS equipment sourcing, supporting regional price stability and service continuity.

3.13.5 IMPACT ON END-USE INDUSTRIES

- BFSI:
  - MSS costs have surged for banks due to tariffs on firewalls, HSMs, and log collection gear.
  - Institutions are adopting SaaS-based SIEM and MDR to reduce CapEx and speed deployment.
  - Multi-year MSS contracts with price-lock or indexed pricing are being structured for predictability.
  - Demand is rising for open-source SOC frameworks to reduce vendor lock-in and tariff exposure.

- Government & Public Sector:
  - Governments are investing in sovereign, locally hosted MSS platforms to protect sensitive data.
  - Domestic SOC development is accelerating to mitigate exposure to tariff volatility.
  - Strategic deals with tariff-exempt MSSPs are being pursued to maintain service continuity.
  - Many are frontloading procurement of compliant security gear ahead of future tariff rounds.
- Manufacturing and Utilities:
  - OT/ICS-focused MSS deployments face delays and cost spikes due to imported sensor and router tariffs.
  - MSSPs are leveraging AI-based anomaly detection to reduce reliance on NDR hardware.
  - Hybrid MSS models (cloud + on-prem) are being adopted to balance performance and cost.
  - Sector-wide efforts are underway to redesign MSS frameworks with fewer hardware refresh dependencies.

3.14 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS

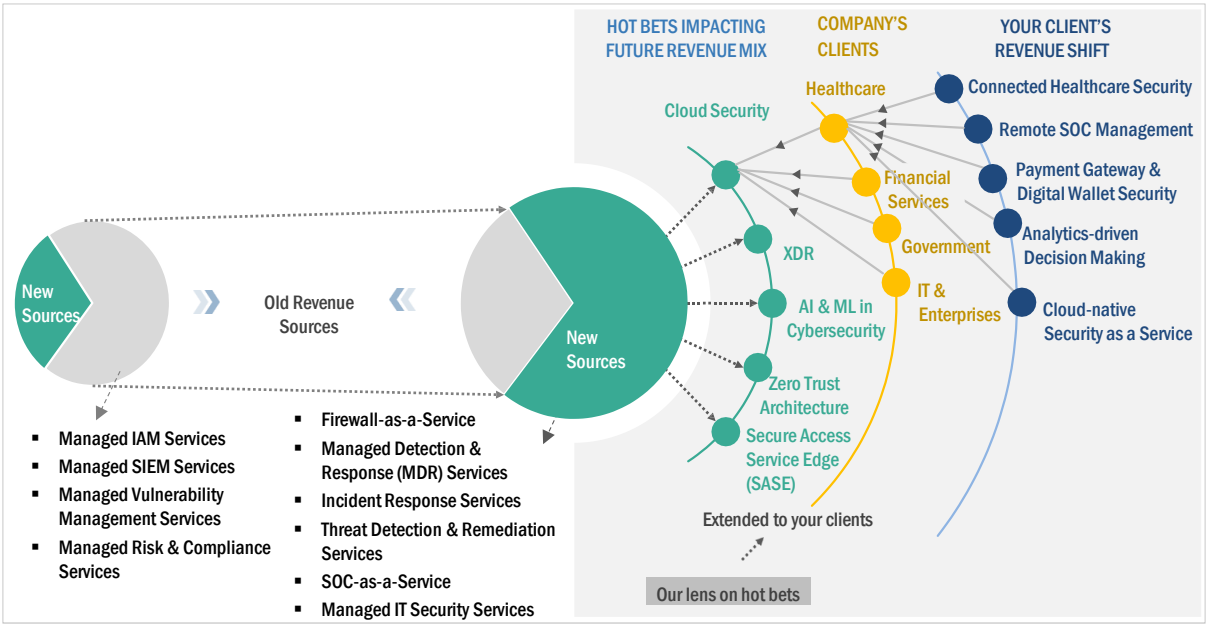
The MSS market is undergoing rapid transformation as enterprises globally shift toward hybrid infrastructure, remote operations, and cloud-first strategies. Organizations are enhancing their cybersecurity posture while reducing operational complexity and cost. The convergence of advanced technologies such as AI, machine learning, automation, behavioral analytics, and zero-trust architecture is redefining how threats are detected, prevented, and responded to in real time.

MSS providers are integrating AI and ML capabilities into their threat detection and response tools, enabling faster incident resolution, predictive analytics, and automated remediation. These advancements are being adopted across critical sectors, including healthcare, BFSI, government, IT and ITeS, and retail, where real-time security intelligence and compliance are essential for business continuity. With the increasing frequency of cyberattacks, particularly ransomware and phishing campaigns, MSSPs are helping clients establish more agile and resilient security frameworks. Cloud-native and software-defined security services are gaining popularity as enterprises look to secure their evolving networks without relying heavily on physical infrastructure.

The rise of remote work and the Bring Your Own Device (BYOD) culture has expanded the attack surface for enterprises, intensifying the demand for endpoint security, identity-based access control, and zero-trust network access (ZTNA). MSSPs are leveraging mobile device management (MDM), remote SOCs (Security Operations Centers), and behavioral analytics to secure remote workforces and third-party access points.

In the financial services and payments sectors, MSSPs are enabling secure digital transformation by offering encrypted data protection, secure APIs, and AI-based fraud detection. As online payment systems, digital wallets, and real-time transactions become more prevalent, MSS solutions are being embedded within financial platforms to ensure end-to-end transaction security and regulatory compliance. Retail and healthcare are adopting MSS solutions not just for protection, but to support secure expansion into cloud environments, edge computing, and IoT deployments.

FIGURE 16 MANAGED SECURITY SERVICES MARKET: TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.15 MANAGED SECURITY SERVICES MARKET: BUSINESS MODELS

TABLE 17 MANAGED SECURITY SERVICES MARKET: BUSINESS MODELS

BUSINESS/ REVENUE MODEL	DESCRIPTION	EXAMPLES OF COMPANIES
Subscription Model	Organizations pay a monthly recurring or annual fee for a pre-defined set of security services, functionalities, and user/device coverage.	Accenture: Offers bundled MSS plans under fixed recurring contracts IBM: Delivers subscription-based threat monitoring and incident response
Pay-as-you-go	Organizations pay only for the services they use, typically billed per user/device or data volume.	Palo Alto Networks: Provides usage-based billing for MSS on its cloud-native platform CrowdStrike: Charges per endpoint and data usage levels
Tiered Pricing Model	Organizations choose from multiple service tiers (basic to premium) with increasing levels of features and support.	Secureworks: Offers scalable tiered MSS packages tailored to enterprise size and risk posture Atos: Provides modular service levels across geographies
Outcome-Based Model	Clients pay based on the achievement of specific security outcomes or KPIs such as threat detection or response time.	Trustwave: Uses a performance-driven model linked to SLAs and incident response Capgemini: Aligns billing with achieved security outcomes in compliance-driven sectors
Hybrid Model	Combines subscription and pay-as-you-go elements, allowing flexible pricing based on usage and service scope.	Orange Cyberdefense: Offers fixed subscription plans with optional pay-per-event add-ons Fujitsu: Delivers hybrid pricing to meet dynamic enterprise security needs

Source: Secondary Research and MarketsandMarkets Analysis

3.16 KEY CONFERENCES & EVENTS IN 2025

This section includes upcoming key conferences and events related to the MSS market in the forthcoming months.

TABLE 18 MANAGED SECURITY SERVICES MARKET: LIST OF KEY CONFERENCES & EVENTS, 2025

YEAR/ QUARTER	NORTH AMERICA	EUROPE	ASIA PACIFIC	REST OF THE WORLD
Q3'25	*[July] Black Hat Cybersecurity Training-US [August] DEF CON 33	[September] Managed Services Summit London 2025 *[September] Gartner Security & Risk Management Summit	-	-
Q4'25	[October] Techno Security & Digital Forensics Conference *[November] FutureCon Boston CyberSecurity Conference-2025 [November] Aspen Cyber Summit-2025 *[December] Cybersecurity Summit US-2025 *[December] Gartner Identity & Access Management Summit-2025	[October] MSP Global 2025 [October] Les Assises de la cybersécurité-2025 [December] CIO Summit 2025	[October] Kaseya DattoCon - 2025 [October] Cyber Security World Asia [November] CODE BLUE 2025	[December] Black Hat Middle East and Africa

** indicates conferences and events that may be more important because of wider reach, sponsorship from leading organizations, thought leadership, etc.*

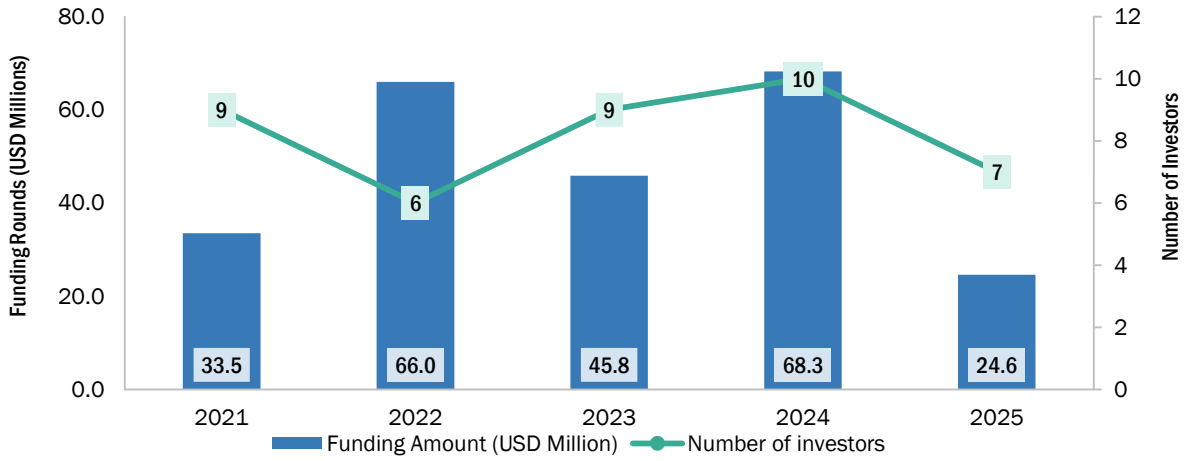
Source: Secondary Research and MarketsandMarkets Analysis

3.17 INVESTMENT AND FUNDING SCENARIO

The managed security services market is witnessing steady investment momentum, driven by the rising need for advanced cybersecurity solutions in an increasingly complex digital landscape. Organizations across industries are channeling funds into MSS startups and SMEs to strengthen capabilities in threat detection, vulnerability management, identity protection, and regulatory compliance. The market has seen strong funding rounds in recent years, with peak inflows in 2022 and 2024, underscoring investor confidence in the sector's long-term growth potential.

Increasing cybersecurity threats, the adoption of cloud and remote work models, and heightened regulatory scrutiny are key factors encouraging capital inflows into MSS providers. With continuous advancements in managed detection and response (MDR), SIEM, and compliance-driven services, the MSS market is poised to attract further investments, fostering innovation, scalability, and broader adoption across enterprises worldwide.

FIGURE 17 NUMBER OF INVESTORS AND FUNDING ROUNDS BY LEADING GLOBAL MANAGED SECURITY SERVICES STARTUPS AND SMES, 2021–2025



Source: Tracxn

4 COMPETITIVE LANDSCAPE

This chapter provides a broad understanding of the competitive leadership mapping of vendors in the MSS market. The competitive landscape also includes the company evaluation matrix of the key vendors and startups/SMEs operating in the MSS market to understand each player's performance. The study covers developments and strategic initiatives undertaken from January 2023 to July 2025.

4.1 KEY PLAYER STRATEGIES/RIGHT TO WIN

Key players in the market have adopted organic and inorganic growth strategies to expand their global presence, which has supported them in increasing their market share. Major market players generate significant revenue from the North American region.

TABLE 19 OVERVIEW OF STRATEGIES ADOPTED BY KEY MANAGED SECURITY SERVICES VENDORS

KEY PLAYER	PRODUCT TYPE	STRATEGIC DEVELOPMENT/ PARTNERSHIP	MERGER & ACQUISITION/ PRODUCT LAUNCH	REGIONAL REVENUE INSIGHT
Accenture	Managed detection & response, Zero Trust, identity & data protection, cloud MSS	Expanded collaboration with Microsoft, AWS, and Google Cloud; partnered with CrowdStrike and Palo Alto Networks for MDR/Zero Trust	Acquired Symantec's Cyber Security Services (from Broadcom); launched AI-driven enhancements in Fusion SOC platform	North America contributed ~45% of security revenues
IBM	IAM, SIEM (QRadar), cloud & data security, threat intelligence MSS	Deepened AI collaboration with Palo Alto Networks; expanded MSS partnerships with AWS and Microsoft Azure	Launched IBM ATOM (AI agentic threat triage/remediation); extended QRadar Suite integrations into MSS	The Americas accounted for ~33% of total security revenues
Deloitte	Managed SOC, compliance monitoring, risk & governance, managed identity security	Strengthened alliances with ServiceNow and Splunk; expanded cloud & OT security services in BFSI & government sectors	Acquired European MSS firm to expand SOC footprint; launched managed compliance-as-a-service platform	The US contributed >40% of Deloitte's MSS revenue
NTT	AI-native SOC, identity (Entra ID), network security MSS, OT/ICS MSS	Partnered with Microsoft to integrate Entra ID into MSS; expanded SOC network across APAC	Launched AI-powered Global Threat Intelligence Center; introduced OT/ICS MSS packages for manufacturing & utilities	APAC contributed ~50% of MSS revenue, followed by EMEA
DXC Technology	Managed network & cloud security, OT/ICS, SD-WAN MSS, compliance MSS	Partnered with Palo Alto Networks and Zscaler to enhance SASE and industrial MSS	Introduced OT/ICS SOC platform for critical infrastructure; expanded managed email & cloud application security offerings	North America ~38% of security revenues, followed by Europe

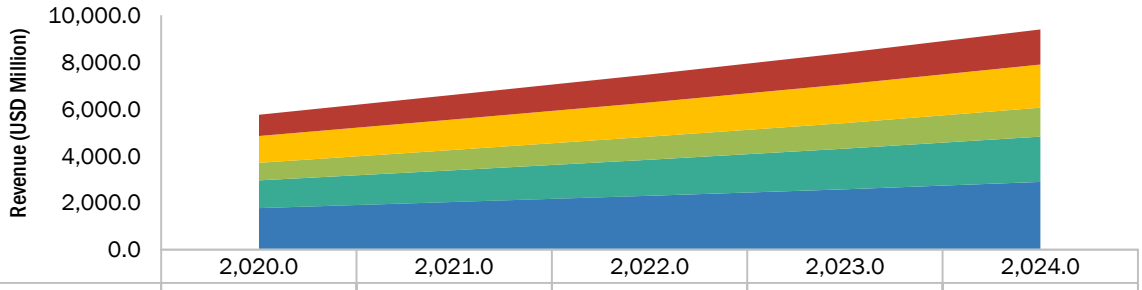
Source: Company Websites and Secondary Sources

4.2 REVENUE ANALYSIS, 2020–2024

The global managed security services (MSS) market has witnessed steady revenue growth between 2020 and 2024, driven by rising cyber threats, increasing regulatory compliance demands, and growing enterprise adoption of managed security solutions. Among the top players, Accenture led the market in 2024 with an estimated USD 2.9 billion in MSS revenue, followed by IBM (USD 1.93 billion) and Deloitte (USD 1.85 billion).

The market remains competitive, with vendors focusing on service innovation, cloud-based security offerings, and expanding their global presence to strengthen their market positioning. According to the analysis, MSS revenues for leading vendors have grown at a CAGR of ~13% during the period and are expected to continue rising as demand for proactive threat detection and response services accelerates.

FIGURE 18 REVENUE ANALYSIS OF TOP FIVE PLAYERS, 2020–2024 (USD MILLION)



	2,020.0	2,021.0	2,022.0	2,023.0	2,024.0
NTT	919.1	1,054.3	1,192.6	1,338.7	1,499.0
Deloitte	1,135.3	1,302.4	1,473.2	1,653.7	1,851.7
DXC Technology	756.9	868.2	982.1	1,102.5	1,234.5
IBM	1,189.4	1,364.4	1,543.3	1,732.4	1,939.9
Accenture	1,778.0	2,039.7	2,307.2	2,589.9	2,900.0

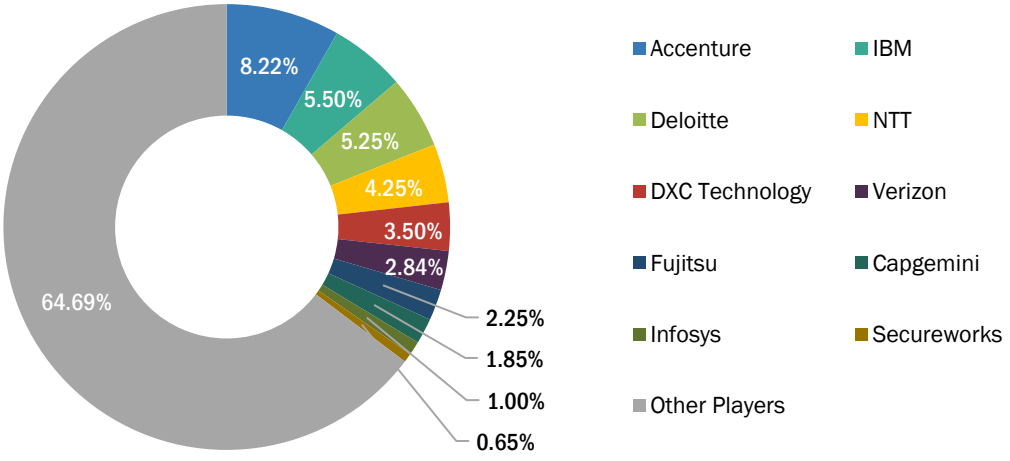
Note: Key players' market share is assessed based on their product offerings and business strategies.

Secondary research and in-depth primary interviews with key industry leaders have also contributed to the analysis.

Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

4.3 MARKET SHARE ANALYSIS, 2024

FIGURE 19 MANAGED SECURITY SERVICES MARKET: SHARE OF LEADING COMPANIES, 2024



Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 20 MANAGED SECURITY SERVICES MARKET: DEGREE OF COMPETITION

COMPANY	MARKET SHARE, 2024
Total Market Share of Top 10 Players	35.31%
Accenture	8.22%
IBM	5.50%
Deloitte	5.25%
NTT	4.25%
DXC Technology	3.50%
Verizon	2.84%
Fujitsu	2.25%
Capgemini	1.85%
Infosys	1.00%
Secureworks	0.65%
Other Players	64.69%

Note: The market share of key players is estimated to be based on their product offerings and business strategies.

Secondary research and in-depth primary interviews with key industry leaders have also contributed to the analysis.

Source: Annual Reports, Press Releases, Investor Presentations, Interviews with Experts, and MarketsandMarkets Analysis

THE DEGREE OF COMPETITION IS DEFINED AS BELOW:

- Fragmented: When the top five players have a total market share of < 25%
- Competitive: When the top five players have a total of 25–50% market share
- Consolidated: When the top five players have a total market share of > 50%

The total market share of the top five players is 26.72%, which is a sign of a competitive market. The top 10 key players contributing to around 35.31% of the total market share are Accenture, IBM, Deloitte, NTT, DXC Technology, Verizon, Fujitsu, Capgemini, Infosys, and Secureworks. Below is a brief description of these top five vendors:

Accenture:

Accenture is a global professional services firm that provides consulting, technology, and outsourcing services, with a strong focus on cybersecurity. Its managed security services (MSS) division offers managed detection and response, Zero Trust frameworks, identity and data protection, cloud security, and risk & compliance services. Accenture's cybersecurity practice is integrated with its global consulting and advisory business, enabling large enterprises in BFSI, government, manufacturing, and healthcare to address regulatory and operational risks. With multiple Fusion Security Operations Centers (SOCs) worldwide, Accenture serves clients across North America, Europe, Asia Pacific, and emerging markets. The company employs more than 740,000 people globally, with thousands dedicated to cybersecurity.

IBM:

IBM is a global technology and consulting company with a well-established cybersecurity division. Its MSS portfolio includes SIEM (QRadar), IAM, threat intelligence, cloud and hybrid security, and data protection services. IBM has invested heavily in AI-driven cybersecurity, launching IBM ATOM and integrating its Watson AI capabilities for SOC automation. The company collaborates with Palo Alto Networks, Microsoft Azure, and AWS to strengthen cloud-native security. IBM's cybersecurity services are adopted across financial services, government, healthcare, and critical infrastructure industries. With operations in over 170 countries, IBM derives about one-third of its security revenue from the Americas. The company employs approximately 315,000 people, including a large global security team.

Deloitte:

Deloitte is one of the "Big Four" professional services firms and a global leader in risk and cybersecurity consulting. Its MSS division is focused on managed SOC services, regulatory compliance monitoring, managed identity security, and governance, risk, & compliance (GRC) solutions. Deloitte's strength lies in regulated industries such as BFSI, energy, and government, where it integrates consulting with managed cybersecurity offerings. The company has invested in partnerships with ServiceNow and Splunk to enhance its compliance-driven MSS portfolio. Deloitte operates across the Americas, EMEA, and APAC, with more than 457,000 employees globally, of which thousands are in cybersecurity and risk services.

NTT:

Nippon Telegraph and Telephone Corporation (NTT) is one of the largest telecommunications and IT services providers globally, with a significant MSS business through NTT Security and NTT Data. Its MSS offerings include AI-native SOC operations, identity security (Microsoft Entra ID), managed network and perimeter security, and OT/ICS security services. NTT has a particularly strong presence in Asia Pacific, providing SOC coverage and threat intelligence services to enterprises across telecommunications, manufacturing, and utilities. It operates a global network of SOCs and threat intelligence centers and serves clients in more than 50 countries. NTT Group employs over 330,000 people worldwide, with cybersecurity being a key growth area.

DXC Technology:

DXC Technology is a global IT services company that delivers managed IT and cybersecurity solutions to enterprises. Its MSS portfolio focuses on managed network and cloud security, OT/ICS protection, secure SD-WAN, risk & compliance monitoring, and managed email and application security. DXC has specialized offerings for industrial and critical infrastructure clients in energy, utilities, and manufacturing. The company partners Palo Alto Networks and Zscaler to expand its SASE and industrial MSS capabilities. With operations in the Americas, Europe, and APAC, DXC employs approximately 130,000 people, with a strong emphasis on enterprise digital transformation and cybersecurity as a growth driver.

4.4 BRAND/PRODUCT COMPARISON

This section provides a comparative analysis of leading MSS vendors based on product portfolio, innovation readiness, customer feedback, and strengths. It highlights how Accenture, IBM, Deloitte, NTT, and DXC Technology differentiate themselves through service offerings, technology integration, and market positioning. The section highlights vendor-specific strategies, wherein Accenture leads with AI-driven security and advisory services, IBM focuses on hybrid cloud integration and AI-powered tools, Deloitte excels in compliance-driven consulting, NTT strengthens its SOC operations and APAC presence, while DXC Technology emphasizes managed cloud and enterprise-scale security solutions.

FIGURE 20 MANAGED SECURITY SERVICES MARKET: COMPARISON OF VENDOR BRANDS

PARAMETERS	accenture	IBM	Deloitte.	NTT	DXC TECHNOLOGY
PRODUCT PORTFOLIO	●	●	●	◔	◔
INNOVATION READINESS	●	◔	◔	◔	◔
CUSTOMER FEEDBACK /RATING	●	◔	◔	◔	◐
STRENGTHS	Strong focus on AI-driven threat detection, Zero Trust adoption, and MDR services Deep integration with advisory and professional services enhances end-to-end security posture	Strong heritage in enterprise security and networking, backed by QRadar SIEM and IBM Cloud Security Established MSS footprint across regulated industries with hybrid and on-premises capabilities Comprehensive integration with AI (Watson) and orchestration tools	Trusted brand in MSS for highly regulated verticals (BFSI, Government) Strong consulting-driven cybersecurity and compliance portfolio Expanding MDR and identity-focused MSS services; positioned among the top 5 MSSPs globally	Leading AI-native SOC operations and integration with Entra ID for identity security Deep presence in APAC markets, with strong network infrastructure security and managed SOC services	Robust MSS portfolio with focus on OT/ICS and secure SD-WAN Positioned well for industrial and critical infrastructure security services Expanding managed cloud security and compliance services for enterprises
WEAKNESSES	Limited proprietary security platform assets compared to tech-centric rivals Heavy reliance on service-driven revenue, with smaller recurring MSS product portfolio than platform-native competitors	Slower cloud-native MSS transition compared to hyperscaler-driven vendors Customer feedback indicates complexity in integrating legacy IBM tools with newer MSS offerings	Innovation pace in MSS perceived slower vs. product-native vendors Heavy reliance on professional services; MSS offerings less standardized globally compared to peers	Limited proprietary hardware/software portfolio; dependency on partner technologies Comparatively weaker North America presence vs. Accenture/IBM	Limited breadth in endpoint and SaaS-layer MSS offerings compared to competitors Lower innovation velocity in identity and email security MSS segments

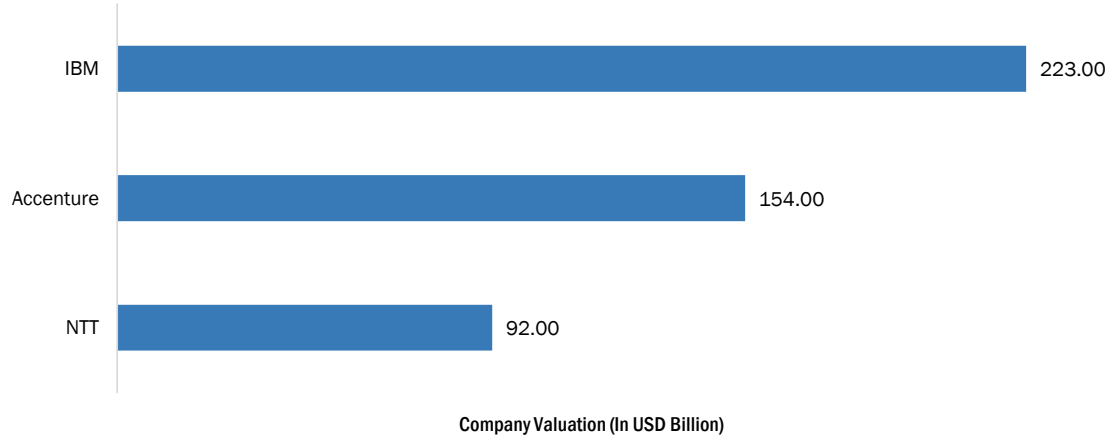
● EXCELLENT | ◔ GOOD | ◐ FAIR | ◔ POOR

Source: Annual Reports, Press Releases, and MarketsandMarkets Analysis

4.5 COMPANY VALUATION AND FINANCIAL METRICS

4.5.1 COMPANY VALUATION

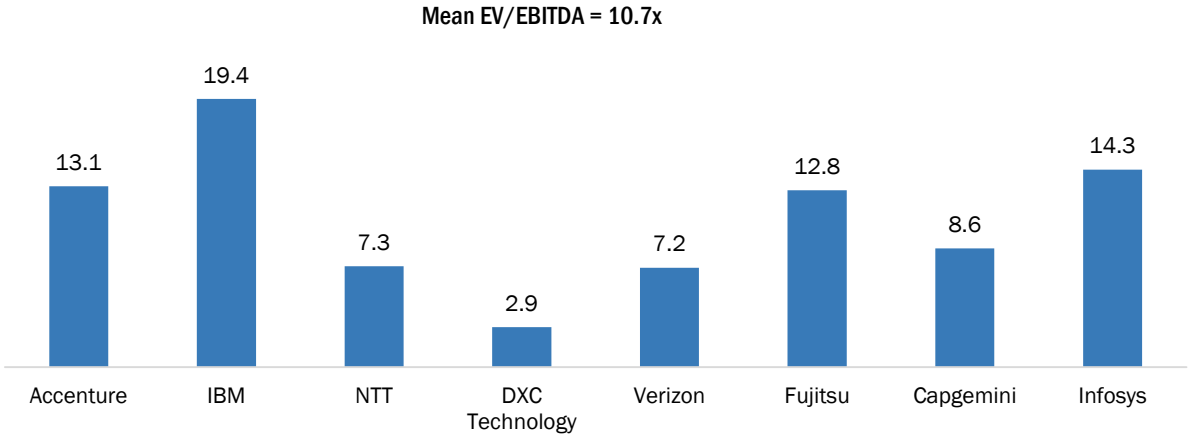
FIGURE 21 MANAGED SECURITY SERVICES MARKET: COMPANY VALUATION OF KEY VENDORS (USD BILLION), 2025



Source: dealroom.co

4.5.2 FINANCIAL METRICS OF KEY VENDORS

FIGURE 22 MANAGED SECURITY SERVICES MARKET: FINANCIAL METRICS OF KEY VENDORS, 2025



Note: EV/EBITDA has been evaluated as of August 17, 2025.

Source: Finbox.com

4.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2024

The company evaluation matrix provides information about the key players offering MSS globally. It also presents the findings and analysis of how well each market vendor performs according to the established competitive leadership mapping criteria. The vendor evaluations are based on two broad categories: product footprint and market share/rank. Each category carries various criteria based on which vendors have been evaluated. The evaluation criteria considered under the product footprint include the breadth and depth of product offerings, product features and functionality, and estimated product revenue. Based on a questionnaire, extensive secondary and primary research was conducted to gather critical information about the vendor's strength of product portfolio and market share/rank. A scale of 0–10 was formulated for each question, after which each criterion for every vendor was scored based on the collected information. After data gathering and verification, the scores and weightage for shortlisted vendors against each parameter were finalized. A comparison scorecard was prepared after evaluating all vendors, and they were then placed into four categories based on their performance in each criterion. These are Stars, Emerging Leaders, Pervasive Players, and Participants.

- Stars: Companies with a large market share, wider application, and geographical use cases and footprint
- Emerging Leaders: Companies with a large market share, low application, and regional penetration
- Pervasive Players: Companies with small market share, high application, and regional availability; these players' products are available for multiple applications/end-use industries in most regions worldwide
- Participants: A small footprint in the market at a global level but may have a strong presence in one or more sub-regions and/or customer segments.

4.6.1 STARS

Vendors in this category generally receive high scores for most evaluation criteria. They offer a strong portfolio of solutions and services and mark their presence in the MSS market by offering platforms based on consumer requirements. These vendors have undertaken various growth strategies to advance consistently in the market. Accenture, Deloitte, IBM, NTT, Fujitsu, LevelBlue, DXC Technology, Verizon, Secureworks, HPE, F5, and Atos are star players in the MSS market. With a broad and robust network in B2B, these companies account for a significant share of the MSS market.

4.6.2 EMERGING LEADERS

Emerging leaders have consistently generated positive revenue growth in the MSS market and boosted their market position through organic and inorganic ventures. Emerging leaders have established vendors with high market share. They are slowly moving toward focusing more on the strength of their product portfolios compared to competitors. TCS, Infosys, CrowdStrike, Capgemini, Orange Cyberdefense, Rapid7, Trend Micro, and Kudelski Security are recognized as emerging leaders operating in the MSS market. These vendors have an innovative portfolio of solutions and services. These companies' robust business strategy enables them to partner with strong players to expand their market reach. The players have consistently generated positive revenue growth in the MSS market and attained market position by undertaking organic and inorganic growth ventures.

4.6.3 PERVASIVE PLAYERS

Pervasive players have demonstrated substantial product innovations compared to their competitors. These key players have focused product portfolios. However, they do not have robust growth strategies and presence in the MSS market space. They possess innovative and niche solutions to cater to future mobility demands. These companies are concerned about their product portfolio and have a robust potential to build strong business strategies to increase their market share and stay on par with the star players. These vendors have consistently offered MSS market solutions to fulfill customer demands. In this case, Lumen Technologies and Kroll are categorized as pervasive players.

4.6.4 PARTICIPANTS

Participants are vendors with less robust business strategies than established vendors. These companies might be new market entrants and require more time before gaining significant market traction. Most participants need to undertake multiple business strategies to expand their capabilities across regions to offer integrated solutions & services to a wide range of clients. No vendors are identified as participants in this study.

FIGURE 23 MANAGED SECURITY SERVICES MARKET: COMPANY EVALUATION MATRIX (KEY PLAYERS), 2024

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

4.6.5 COMPANY FOOTPRINT: KEY PLAYERS, 2024

4.6.5.1 Company footprint

FIGURE 24 MANAGED SECURITY SERVICES MARKET: COMPANY FOOTPRINT

Company	REGION FOOTPRINT	TYPE FOOTPRINT	VERTICAL FOOTPRINT	OVERALL FOOTPRINT
IBM	○○○○	○○○○	○○○○	○○○○
NTT	○○○○	○○○○	○○○○	○○○○
LevelBlue	○○○○	○○○○	○○○○	○○○○
Accenture	○○○○	○○○○	○○○	○○○○
DXC Technology	○○○○	○○○○	○○○○	○○○○
Deloitte	○○○○	○○○○	○○	○○
Secureworks	○○○○	○○○○	○○	○○
Verizon	○○○○	○○○○	○○	○○
Fujitsu	○○○○	○○○○	○○	○○
HPE	○○○○	○○○○	○○○	○○○
TCS	○○○○	○○○○	○○○○	○○
Atos	○○○○	○○○○	○○○	○○○
Orange Cyberdefense	○○○○	○○○○	○○	○○
Rapid7	○○○○	○○○○	○○	○○
Trend Micro	○○○○	○○○○	○○	○○
Kudelski Security	○○○	○○○○	○○○	○○○
CrowdStrike	○○○	○○○○	○○○	○○○
F5	○○○	○○○○	○○○	○○○
Capgemini	○○○	○○○○	○○○	○○○
Infosys	○○○	○○○○	○○○	○○○
Lumen Technologies	○○○	○○○○	○○○	○○○
Kroll	○○○	○○○○	○○	○○

RATING : ○○○○ EXCELLENT ○○○ GOOD ○○ AVERAGE ○ BELOW AVERAGE NOT APPLICABLE

Source: Press Releases, Investor Presentations, Interviews with Experts, and MarketsandMarkets Analysis

4.6.5.2 Regional footprint

TABLE 21 MANAGED SECURITY SERVICES MARKET: REGIONAL FOOTPRINT

COMPANY	NORTH AMERICA	EUROPE	ASIA PACIFIC	MIDDLE EAST & AFRICA	LATIN AMERICA	REGIONAL FOOTPRINT
IBM	Y	Y	Y	Y	Y	4.00
NTT	Y	Y	Y	Y	Y	4.00
AT&T	Y	Y	Y	Y	Y	4.00
Accenture	Y	Y	Y	Y	Y	4.00
DXC Technology	Y	Y	Y	Y	Y	4.00
Secureworks	Y	Y	Y	Y	N	3.20
Deloitte	Y	Y	Y	Y	Y	4.00
Verizon	Y	Y	Y	Y	N	3.20
Fujitsu	Y	Y	Y	Y	Y	4.00
HPE	Y	Y	Y	Y	Y	4.00
TCS	Y	Y	Y	Y	Y	4.00
Atos	Y	Y	Y	Y	N	3.20
Orange Cyberdefense	N	Y	Y	Y	N	2.40
Rapid7	Y	Y	Y	N	N	2.40
Trend Micro	Y	Y	Y	Y	Y	4.00
Kudelski Security	Y	Y	Y	N	N	2.40
CrowdStrike	Y	Y	Y	Y	Y	4.00
F5	Y	Y	Y	Y	Y	4.00
Capgemini	Y	Y	Y	Y	Y	4.00
Infosys	Y	Y	Y	Y	Y	4.00
Lumen Technologies	Y	N	Y	N	N	2.40
Kroll	Y	Y	Y	Y	Y	4.00

Source: Company Websites and MarketsandMarkets Analysis

4.6.5.3 Type footprint

TABLE 22 MANAGED SECURITY SERVICES MARKET: TYPE FOOTPRINT

COMPANY	FULLY MANAGED SECURITY SERVICES	CO-MANAGED SECURITY SERVICES	TYPE FOOTPRINT
IBM	Y	Y	4.00
NTT	Y	Y	4.00
LevelBlue	Y	Y	4.00
Accenture	Y	Y	4.00
DXC Technology	Y	Y	4.00
Secureworks	Y	Y	4.00
Deloitte	Y	Y	4.00
Verizon	Y	Y	4.00
Fujitsu	Y	Y	4.00
HPE	Y	Y	4.00
TCS	Y	Y	4.00
Atos	Y	Y	4.00
Orange Cyberdefense	Y	Y	4.00
Rapid7	Y	Y	4.00
Trend Micro	Y	Y	4.00
Kudelski Security	Y	Y	4.00
CrowdStrike	Y	Y	4.00
F5	Y	Y	4.00
Capgemini	Y	Y	4.00
Infosys	Y	Y	4.00
Lumen Technologies	Y	Y	4.00
Kroll	Y	Y	4.00

Source: Press Releases and MarketsandMarkets Analysis

4.6.5.4 Vertical footprint

TABLE 23 MANAGED SECURITY SERVICES MARKET: VERTICAL FOOTPRINT

COMPANY	BFSI	GOVERNMENT	HEALTHCARE	TELECOMMUNICATION	IT & ITES	RETAIL & ECOMMERCE	ENERGY & UTILITIES	MANUFACTURING	OTHER VERTICALS	VERTICAL FOOTPRINT
IBM	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
NTT	Y	Y	N	N	Y	Y	Y	N	Y	2.67
AT&T	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Accenture	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
DXC Technology	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Secureworks	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Deloitte	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Verizon	N	Y	N	N	N	Y	Y	N	Y	1.78
Fujitsu	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
HPE	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
TCS	Y	N	Y	N	Y	N	Y	Y	Y	2.67
Atos	Y	N	Y	N	Y	N	Y	Y	Y	2.67
Orange Cyberdefense	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56
Rapid7	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56
Trend Micro	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56
Kudelski Security	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56
CrowdStrike	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56
F5	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56
Capgemini	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Infosys	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56
Lumen Technologies	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56
Kroll	Y	Y	Y	Y	Y	Y	Y	N	Y	3.56

Source: Press Releases and MarketsandMarkets Analysis

4.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2024

The company evaluation matrix for startups and SMEs identifies and profiles companies with commercial MSS offerings globally, regardless of their development stage (seed, early-stage, mid-stage, etc.). Companies are classified into startups and SMEs based on defined parameters:

SMEs (Small & Medium-sized Enterprises):

- Companies with an overall annual revenue of less than USD 500 million

Startups:

- The annual revenue is less than USD 50 million
- The employee count is less than 100
- Company valuation is less than USD 500 million
- The age of the company is less than 10 years, and any of the above conditions are met

The startup/SME evaluation matrix features emerging and innovative MSS market companies. The startups selected for the matrix were chosen based on their founding years, revenues, and employee count. Overall vendor evaluations are based on the strength of the product portfolio and market shares/rank.

- Progressive Companies: These vendors have been making their presence in the market by offering innovative solutions based on customer requirements and adopting various strategies to achieve market growth.
- Responsive Companies: These companies have the potential to build strong business strategies, expand their product footprint, and stay on par with progressive companies.
- Dynamic Companies: They offer innovative solutions portfolios and have competent distribution to increase their market presence.
- Starting Blocks: Most starting blocks have been undertaking multiple product developments and launches to cater to a broader range of clients.

4.7.1 PROGRESSIVE COMPANIES

These companies have performed exceedingly well in product and business excellence parameters. They have a robust partner ecosystem and well-developed marketing channels and have received extensive funding to develop their product portfolio. These companies have been instrumental in achieving their growth prospects, thereby attaining high partner attractiveness. Trustwave, LightEdge, LRQA, DigitalXRAID, TrustNet, SecurityHQ, Cipher, and CyFlare are progressive companies in the MSS market.

4.7.2 RESPONSIVE COMPANIES

RSI Security, Avertium, Secnap, Netsurion, and Teceze have performed well in the market share/rank parameter and fall under this category. They focus on specific technology related to the product or service offered. These companies have a smaller product footprint than other companies.

4.7.3 DYNAMIC COMPANIES

These startups and SMEs have performed well in the product portfolio parameter. However, they rank slightly lower in market share compared to more progressive and responsive companies. They generally focus on a specific technology related to the product or service offering. Atlas Systems and Ascend Technologies are considered dynamic companies in the MSS market.

4.7.4 STARTING BLOCKS

These players with niche offerings are expected to start gaining their position in the market. They have less business excellence and product excellence than other established start-ups. However, they can always gain a chance to consolidate their market space. They may be new entrants in the market and need more time to gain significant traction. No vendor is identified in this category.

FIGURE 25 MANAGED SECURITY SERVICES MARKET: COMPANY EVALUATION MATRIX (STARTUPS/SMES), 2024

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

4.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2024

4.7.5.1 Detailed list of key startups/SMEs

TABLE 24 MANAGED SECURITY SERVICES MARKET: KEY STARTUPS/SMES

COMPANY NAME	CATEGORY	OWNERSHIP STATUS	HQ LOCATION	FOUNDING YEAR	EMPLOYEE COUNT	FINANCING ROUND	LATEST FUNDING ROUND	TOTAL FUNDING (USD MILLION)
Cipher	IT service management company	Private	Miami, Florida US	2000	201-500	-	-	-
RSI Security	IT Services and IT Consulting	Private	San Diego, California	2008	51-200	-	-	-
SecurityHQ	IT Services and IT Consulting	Private	London	2003	201-500	-	-	-
LightEdge	IT Services and IT Consulting	Private	Des Moines, Iowa	1996	51-200	Angel Investors	Seed	21.2
LRQA	IT Services and IT Consulting	Private	Birmingham, England	2003	201-500	-	-	-
Teceze	Computer and Network Security	Private	London, England	2012	51-200	-	-	-
CyFlare	Computer and Network Security	Private	Rochester, NY	2017	11-50	-	-	-
Ascend Technologies	IT Services and IT Consulting	Private	Chicago, Illinois	2020	201-500	Venture Capital-Backed	Series A	35.5
Avertium	Computer and Network Security	Private	Phoenix, Arizona	2019	201-500	-	-	-
DigitalXRAID	Computer and Network Security	Private	Doncaster, South Yorkshire	2015	51-200	Private Equity	-	-
TrustNet	Computer and Network Security	Private	Atlanta, Georgia	2005	51-200	-	-	-

Source: Press Releases and MarketsandMarkets Analysis

4.7.5.2 Competitive benchmarking of key startups/SMEs

TABLE 25 MANAGED SECURITY SERVICES MARKET: COMPETITIVE BENCHMARKING OF KEY STARTUPS/SMES

	TYPE		VERTICAL									REGION				
COMPANY NAME	FULLY MANAGED	CO-MANAGED	BFSI	GOVERNMENT	HEALTHCARE	TELECOMMUNICATIONS	IT & ITES	RETAIL & ECOMMERCE	ENERGY & UTILITIES	MANUFACTURING	OTHER VERTICALS	NORTH AMERICA	EUROPE	ASIA PACIFIC	MIDDLE EAST & AFRICA	LATIN AMERICA
Cipher	Y	Y	Y	N	Y	N	N	N	Y	N	Y	Y	Y	N	N	Y
RSI Security	Y	Y	Y	Y	Y	N	Y	N	N	N	Y	Y	N	N	N	N
SecurityHQ	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
LightEdge	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	N	N	N
LRQA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Teceze	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N
CyFlare	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
Ascend Technologies	Y	Y	Y	Y	Y	N	Y	N	N	Y	Y	Y	N	N	N	N
Avertium	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
DigitalXRAID	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N
TrustNet	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	N	N	N	N

Source: Press Releases and MarketsandMarkets Analysis

4.8 COMPETITIVE SCENARIO

The competitive scenario includes the recent developments of key players operating in the global MSS market. The market share analysis of key players has been done based on the following parameters: depth of product range and revenues generated. Additionally, the competitive landscape studies the key growth strategies adopted by the market players between 2023 and 2025 to increase their global presence and shares in the MSS market.

4.8.1 PRODUCT LAUNCHES & DEVELOPMENTS

The top 5 companies have adopted the new product launches and developments strategy to improve their product offerings and provide better solutions to enterprise clients.

TABLE 26 MANAGED SECURITY SERVICES MARKET: PRODUCT LAUNCHES & DEVELOPMENTS, JANUARY 2023-JULY 2025

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
May 2025	Product Launch	IBM (US)	QRadar Investigation Assistant (Solution)	IBM launched the QRadar Investigation Assistant, an AI-powered tool integrated into QRadar SIEM to enhance MSS operations. It uses watsonx to automate offense summaries, reduce false negatives, and deliver actionable recommendations, thus boosting analyst productivity and response speed.
April 2025	Product Enhancement	IBM (US)	IBM z17 (Service)	IBM upgraded its z17 platform with AI-powered threat detection, data classification, and quantum-safe crypto tools to bolster its managed security services (MSS), enhancing threat response, compliance, and data security.
April 2025	Product Launch	IBM (US)	Autonomous Threat Operations Machine (Solution)	IBM expanded its managed detection and response capabilities with ATOM, a multi-agent AI framework that autonomously triages, investigates, and remediates threats and PTI, which delivers predictive, vertical-specific threat intelligence. These agentic enhancements drive proactive and autonomous security operations.
February 2025	Product Launch	NTT (Japan)	Private 5G Security Service (Service)	NTT launched a managed security service for private 5G/OT environments, combining Palo Alto Networks NGFW and ML-based threat detection to enforce zero-trust access.
December 2024	Product Enhancement	LevelBlue (US)	LevelBlue USM Anywhere (Solution)	USM Anywhere is an XDR platform with new authentication, compliance reports, cloud connectors, OTX enrichment, BlueApps integrations, and enhanced threat tracking.
November 2024	Product Enhancement	Accenture (Ireland)	Generative AI Cybersecurity Services (Service)	Accenture enhanced its MSS by integrating generative AI capabilities. The update includes advanced deepfake protection and quantum-safe data security features. These additions aim to improve threat detection, response efficiency, and long-term data resilience.
October 2024	Product Launch	IBM (US)	IBM Security Connect (Solution)	IBM introduced Security Connect, a cloud-native integration platform that empowers MSS operations by centralizing analytics, sharing threat data, and enabling app connectivity across security tools (e.g., SIEM, SOAR, XDR). It enhances cross-platform correlation, improves security workflows, and supports federated visibility in managed environments.

October 2024	Product Launch	LevelBlue (US)	Managed Threat Detection & Response (Service)	LevelBlue launched MTDR service for MSPs/MSSPs via USM Anywhere platform, offering 24/7 threat monitoring and incident response.
October 2024	Product Launch	LevelBlue (US)	Vulnerability Management (Service)	Vulnerability scanning and remediation prioritization are integrated into the MSS platform for continuous risk mitigation.
October 2024	Product Launch	LevelBlue (US)	Managed Endpoint Security (Service)	Endpoint protection service detects, prevents, and responds to endpoint-based threats for MSSP customers.
September 2024	Product Launch	LevelBlue (US)	MTDR for Government (Service)	LevelBlue launched managed threat detection and response specifically for the US government entities, delivering 24/7 threat monitoring and response.
August 2024	Product Launch	IBM (US)	IBM Consulting Cybersecurity Assistant (Service)	IBM launched the IBM Consulting Cybersecurity Assistant, a generative AI tool within its threat detection and response services. Built on watsonx, it accelerates threat investigations, automates analyst tasks, and enhances SOC efficiency with historical threat correlation, auto-recommended actions, and a conversational AI engine that improves security posture and reduces response times.
August 2024	Product Launch	IBM (US)	IBM Sterling Secure Proxy (Service)	IBM launched Sterling Secure Proxy under its MSS portfolio to secure multi-enterprise data exchanges. Positioned in the DMZ, it blocks direct access to internal servers during B2B and MFT transactions. Key MSS features include multifactor authentication, SSL session breaks, malware scanning, and protocol inspection to strengthen perimeter security and reduce risk.
August 2024	Product Launch	IBM (US)	Threat Detection and Response Services (Service)	IBM launched a new generative AI-powered cybersecurity assistant designed to enhance its threat detection and response services. This assistant streamlines security operations and improves threat identification and response. It utilizes historical correlation analysis and a conversational engine to accelerate investigations and automate operational tasks, significantly reducing alert investigation times for clients.
July 2024	Product Enhancement	NTT (Japan)	WideAngle MSS (Service)	NTT enhanced its WideAngle Managed Security Service by integrating Netskope's cloud-based SASE platform for advanced proxy analysis. This integration boosts real-time threat visibility across cloud, web, and private applications, enriching NTT Com's SIEM-based monitoring with AI/ML-powered insights. The collaboration strengthens defense-in-depth and zero-trust implementation for hybrid IT environments.

June 2024	Product Enhancement	NTT (Japan)	SamurAI MDR (Service)	NTT introduced SamurAI MDR, a next-gen MDR service powered by the Open Threat Detection & Response platform. It delivers 24/7 threat detection, response, and hunting across cloud, endpoint, network, and OT environments.
June 2024	Product Enhancement	NTT (Japan)	Qualys-powered MSS (Service)	NTT integrated Qualys Cloud Platform into NTT Security's MSS offerings to standardize asset inventory, vulnerability management, compliance, and web app security capabilities.
November 2023	Product Launch	IBM (US)	IBM QRadar SIEM (Solution)	IBM QRadar SIEM was launched as a cloud-native security information and event management system designed for hybrid cloud environments. It would integrate advanced AI capabilities for efficient threat detection and response, targeting noise reduction and improvement of alert quality. The platform offered streamlined operations for security teams, enabling faster identification and management of cybersecurity threats in diverse IT landscapes. This evolution in IBM's cybersecurity suite would underscore a commitment to enhance digital security in an era increasingly reliant on hybrid cloud solutions.
October 2023	Product Launch	IBM (US)	IBM Threat Detection and Response Services (TDR) (Service)	IBM's TDR Services provided round-the-clock monitoring, investigation, and automated remediation of security alerts across hybrid cloud environments. These services leveraged advanced AI models for effective threat management, capable of handling up to 85% of alerts, significantly accelerating the response times. The TDR services were designed for integration with existing security tools and cloud, on-premises, and operational technologies. Key features included crowdsourced detection rules, optimized alerts, MITRE ATT&CK assessment, seamless integration across security assets, and 24×7 global support. These services bolster organizations' cybersecurity postures by simplifying and enhancing threat detection and response capabilities.
July 2023	Product Launch	NTT (Japan)	MDR service (Service)	NTT launched an outsourcing service for security management (MDR service) to prevent incidents and minimize damage when incidents occur. The service was introduced in Japan in July 2023 and expanded worldwide within the fiscal year ending in March 2024.
April 2023	Product Launch	IBM (US)	IBM QRadar Suite (Software)	IBM QRadar Suite was launched as an AI-enhanced cybersecurity platform combining threat detection and response tools into a unified system. Key features included QRadar Log Insights, QRadar SIEM, QRadar EDR and extended detection and response (XDR), and QRadar SOAR, all integrated into a single interface. This suite, offered as SaaS on AWS, employed AI for alert triage, enabling security analysts to prioritize critical threats efficiently. Its AI models were specifically trained to

				handle security alerts, streamlining threat management and improving response times. The suite was designed to enhance cybersecurity operations by automating key processes and providing comprehensive threat analysis and response capabilities.
March 2023	Product Launch	NTT (Japan)	MDR security service (Service)	NTT launched MDR security service to help companies achieve business performance objectives through improved cyber resilience. The cloud-native, analytics-driven offering combines human and machine expertise with leading technologies and threat intelligence to reduce the mean time needed to detect and respond to cyber attacks.

Source: Company Websites and Secondary Sources

4.8.2 DEALS

This section comprises deals, including partnerships, collaborations, mergers, and acquisitions of the top 5 vendors. The strategy of partnerships and collaborations accounted for the largest share of the overall growth strategies implemented by key players in the MSS market. Companies have partnered with other players to cater to reputable clients across the globe and mark their presence in their respective regional markets.

Most market players are using mergers & acquisitions as a strategy to expand their customer base and enhance their technological capabilities.

TABLE 27 MANAGED SECURITY SERVICES MARKET: DEALS, JANUARY 2023–JULY 2025

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
June 2025	Acquisition	IBM (US)	Seek AI (US)	IBM acquired Seek AI to support the launch of Watsonx AI Labs in New York, enhancing its agentic AI development for cybersecurity, MSS, and beyond.	NA
May 2025	Collaboration	Accenture (Ireland)	Google (US)	Accenture and Google partnered at RSA 2025 to wrap services around Google Cloud Security (Chronicle, Mandiant), unifying detection, SOAR, and automation into MSS offerings for faster enterprise security modernization.	NA
April 2025	Collaboration	Accenture (Ireland)	CyberArk (US)	Accenture's AI Refinery integrated with CyberArk's Identity Security Platform to extend Zero Trust identity controls to AI agents, enhancing identity protection in MSS environments.	NA
March 2025	Partnership	NTT (Japan)	Rubrik (US)	NTT, through its subsidiary NTT DATA, expanded its global cybersecurity strategy by partnering with Rubrik to offer comprehensive ransomware protection and cyber recovery services. The partnership integrates Rubrik's zero-trust-based cyber-recovery, advisory, implementation, and MSS support across on-prem, SaaS, and cloud environments.	NA

March 2025	Collaboration	NTT (Japan)	CrowdStrike (US)	NTT expanded its managed cybersecurity services by integrating the AI-native CrowdStrike Falcon platform, bringing advanced threat detection, 24/7 threat hunting, and incident response capabilities into its global MSS delivery model.	NA
March 2025	Collaboration	NTT (Japan)	CrowdStrike (US)	NTT expanded its managed cybersecurity services by integrating the AI-native CrowdStrike Falcon platform, bringing advanced threat detection, 24/7 threat hunting, and incident response capabilities into its global MSS delivery model.	NA
March 2025	Strategic Partnership	Accenture (Ireland)	Verizon (US)	Accenture and Verizon Business formed a strategic partnership to co-develop and deliver advanced cybersecurity-as-a-service solutions, including Identity & Access Management, Managed Extended Detection and Response (MxDR), and cyber risk services.	NA
March 2025	Collaboration	Accenture (Ireland)	CrowdStrike (US)	Accenture and CrowdStrike teamed up to integrate Falcon into MxDR, delivering AI-native threat detection, continuous exposure management, and optimized SecOps for MSS clients.	NA
February 2025	Partnership	NTT (Japan)	Palo Alto Networks (US)	NTT and Palo Alto Networks have introduced a managed security service specifically designed for private 5G and operational technology (OT) environments. This service combines Palo Alto's next-generation firewall (NGFW), OT and IoT subscriptions, and machine learning-driven threat detection with NTT's Private 5G infrastructure. The collaboration aims to enhance security by implementing zero-trust principles, increasing visibility, and enabling automated responses to industrial use cases.	NA
January 2025	Partnership	IBM (US)	Palo Alto Networks (US)	IBM and Palo Alto Networks partnered to enhance MSS by integrating Palo Alto's Cortex XSIAM platform with IBM Consulting and security services. This collaboration aims to boost SOC automation, accelerate threat detection, and improve incident response through AI-powered solutions, strengthening IBM's MSS capabilities for modern hybrid cloud environments.	NA
January 2025	Partnership	IBM (US)	Telefónica Tech (Spain)	IBM and Telefónica Tech partnered to integrate quantum-safe cryptography into Telefónica Tech's cybersecurity services as part of its MSS offerings. The collaboration includes deploying IBM's quantum-safe infrastructure at Telefónica Tech's Madrid HQ, enabling enhanced protection against future quantum threats.	NA

December 2024	Partnership	DXC Technology (US)	Blackout Technologies (UK)	DXC Technology partnered with UK-based Blackout Technologies to launch an MSS offering focused on mobile device security and compliance. The solution restricts unauthorized smart device usage during work hours, helping protect sensitive data, meet regulatory requirements (e.g., GDPR, MiFID II, PCI DSS), and improve workforce productivity. It strengthens DXC's MSS portfolio with advanced, context-aware mobile security for financial services and fleet management.	NA
October 2024	Collaboration	NTT (Japan)	Palo Alto Networks (US)	NTT introduced a managed XDR service powered by Palo Alto Cortex XSIAM, delivering cloud-to-edge AI-driven threat detection and automated response across hybrid environments.	NA
July 2024	Acquisition	IBM (US)	SiXworks Limited (UK)	IBM acquired SiXworks Limited, a UK consultancy specializing in secure digital transformation for the defense sector. This acquisition will enhance IBM's capabilities in cybersecurity and digital solutions for the UK public sector and strengthen its support for clients in highly secure environments, including the UK Ministry of Defence.	NA
July 2024	Collaboration	IBM (US)	Microsoft (US)	IBM Consulting and Microsoft collaborated under IBM's Threat Detection & Response Cloud Native MSS to integrate Microsoft Sentinel, Defender XDR, and Defender for Cloud with IBM's SOC services, providing 24/7 monitoring, investigation, and automated remediation.	NA
July 2024	Partnership	Accenture (Ireland)	SandboxAQ (US)	Accenture expanded partnership for enterprise data encryption and quantum-safe security, integrating SandboxAQ's AQtive Guard into MSS for encryption risk assessments and data resilience.	NA
May 2024	Partnership	IBM (US)	Palo Alto Networks (US)	Palo Alto Networks and IBM collaborated in a strategic partnership to deliver AI-powered security solutions, with IBM providing security consulting services across Palo Alto Networks' platforms. This collaboration included acquiring IBM's QRadar SaaS assets by Palo Alto Networks, enhancing threat protection, and streamlining security operations for customers through advanced AI capabilities.	NA
Apr 2024	Collaboration	IBM (US)	Fortinet (US)	IBM Cloud and Fortinet collaborated to offer Fortinet's Virtual FortiGate Security Appliance (vFSA) on IBM Cloud, enhancing workload protection with integrated firewall services for clients operating in hybrid cloud environments.	NA

November 2023	Acquisition	Accenture (Ireland)	Innotec Security (Spain)	Accenture acquired Innotec Security, a privately held company specializing in cybersecurity-as-a-service, cyber resilience, and cyber risk management, expanding its capabilities and footprint in Spain. Innotec Security was previously owned by the parent company, Entelgy Group. The acquisition of Innotec Security, which also came with a presence in Barcelona, Seville, and the Basque Country, would add 500 cybersecurity professionals to Accenture Security's workforce of 20,000 professionals globally, making Accenture Security one of the top managed security services (MSS) players in Spain.	NA
October 2023	Acquisition	Accenture (Ireland)	MNEMO (Mexico)	Accenture acquired MNEMO Mexico, a privately held company specializing in MSS. The company's portfolio included advanced cyber defense and response capabilities, a cyber intelligence platform powered by generative AI and other advanced technologies, and a perennially continuous security operations center in Mexico City. Its client base spanned multiple industries, including telecommunications, banking, and insurance. The addition of MNEMO Mexico's managed cybersecurity services would help Accenture grow its business in Mexico, expand its presence in Latin America, and support the North American business.	NA
June 2023	Partnership Expansion	DXC Technology (US)	Oracle (US)	DXC's expanded ITS partnership with Oracle, enhancing its MSS by strengthening secure cloud management, compliance, and governance capabilities. Through Oracle Cloud Infrastructure (OCI), DXC can deliver MSS offerings such as cloud workload protection, secure application hosting, and risk-reduced cloud migration, supporting enterprise security in hybrid and multi-cloud environments.	NA
May 2023	Acquisition	IBM (US)	Polar Security (Israel)	The acquisition aimed to enhance cloud and SaaS application data security, addressing the issue of shadow data. Polar Security's DSPM technology would be integrated into IBM's Guardium product family, providing comprehensive data security across all data types and storage locations.	USD 60 Million
April 2023	Collaboration	Accenture (Ireland)	Palo Alto Networks (US)	Accenture expanded its cybersecurity collaboration with Palo Alto Networks to offer integrated Prisma SASE solutions covering advisory, implementation, and managed SASE-as-a-service for zero-trust networking.	NA

April 2023	Partnership	Accenture (Ireland)	Google Cloud (US)	Accenture and Google Cloud expanded their global partnership to help businesses protect critical assets and strengthen security against persistent cyber threats. This partnership would focus on Accenture's new MxDR service with security-specific generative artificial intelligence (AI) from Google Cloud, designed to integrate with the most common security technology platforms and other clouds.	NA
March 2023	Collaboration	IBM (US)	Cohesity (US)	This partnership led to the creation of the IBM Storage Defender solution, integrating Cohesity's data protection capabilities. The solution aimed to provide robust defenses against cyber threats such as ransomware and human error, with features AI-driven event monitoring and automated recovery functions.	NA
February 2023	Acquisition	Accenture (Ireland)	Morphus (Brazil)	Accenture acquired Morphus, a Brazil-based cybersecurity company. Morphus had deep expertise in cybersecurity research, cyber defense, and threat intelligence services. The acquisition complemented Accenture's global security practice and accelerated the growth of the cyber industry practice in Latin America.	NA

Source: Company Website and Press Releases

5 COMPANY PROFILES

5.1 DIGITALXRAID

5.1.1 BUSINESS OVERVIEW

DigitalXRAID is a leading MSSP and part of Xypher, a UK-based group of cybersecurity, compliance, digital forensics, and e-Discovery specialists. Together, they bring over a decade of certified expertise, delivering comprehensive support across the full cyber resilience lifecycle. The group comprises over 150 security professionals with experience protecting some of the world's most recognizable brands, including retail, professional sports clubs, healthcare, finance, and universities. Their expertise also supports the UK's critical national infrastructure, including governing bodies, local government, telecommunications, energy, and nuclear power, as well as 60% of the UK's law enforcement agencies, which manage sensitive evidence in high-profile cases.

Through its MSS portfolio, DigitalXRAID helps clients reduce exposure to threats by up to 95%, enhance workforce cyber awareness, and maintain regulatory compliance. The company serves SMEs and large enterprises across multiple sectors, including government, BFSI, healthcare, technology, utilities, energy, and education. It holds numerous certifications, including CREST, CHECK, Cyber Essentials Plus, IASME Gold Standard, ISO 27001, and ISO 9001.

In a significant milestone, DigitalXRAID was acquired by Limerston Capital's cybersecurity platform in July 2025, expanding its MSS and cyber capabilities. This strategic acquisition strengthened 24/7 SOC and MDR operations, incident response, digital forensics, and cyber consultancy services, positioning the company within a larger UK cybersecurity platform to deliver enhanced end-to-end cyber resilience across public and private sectors. DigitalXRAID provides round-the-clock protection, helping organisations safeguard data, prevent breaches, and stay ahead of malicious actors. The company operates primarily across the UK and Europe, while also supporting international clients. Its team members are distributed nationally across the UK & Ireland.

TABLE 28 DIGITALXRAID: COMPANY OVERVIEW

Founding Year	2015
Headquarters Country	UK
Headquarters City	Doncaster, South Yorkshire
Ownership Type	Private (Acquired by Limerston Capital)

Source: Company Website, Annual Reports, and SEC Filings

5.1.2 PRODUCTS/SOLUTIONS/SERVICES OFFERED

TABLE 29 DIGITALXRAID: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Service	Managed Security Operations Centre (SOC)	The Managed Security Operations Centre (SOC) is a fully managed, 24/7 service delivering continuous monitoring, threat detection, investigation, and response. Operated by NCSC, Microsoft and CHECK-certified analysts, it provides real-time visibility and incident handling. It also offers compliance support across on-premises and cloud environments.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation
Service	Incident Response Service	Rapid incident response service provides expert containment, investigation, and remediation during cyber incidents. DigitalXRAID's NCSC and CREST certified specialists minimize business impact through triage, containment, forensic analysis, threat eradication, recovery support, and post-incident reporting with actionable recommendations.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation
Service	Endpoint Detection & Response (EDR)	Endpoint Detection & Response (EDR) is an advanced endpoint monitoring and threat detection service that provides comprehensive protection across workstations, servers, and cloud workloads. It offers continuous visibility, rapid containment, and response to malicious activity. It also reduces dwell time and protects organisations from sophisticated endpoint-based attacks.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation

Service	HarpoonX Managed Phishing Service	HarpoonX Managed Phishing Service is a managed phishing simulation and awareness service that tests employee resilience against social engineering attacks. It delivers realistic phishing campaigns, detailed reporting, and targeted training to reduce human risk and strengthen organisational security culture over time.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation
Service	Managed Microsoft Sentinel Service	Managed Microsoft Sentinel Service is a fully managed Microsoft Sentinel SIEM and SOAR service delivering cloud-native threat detection, log management, and automated response. It includes rule tuning, alert triage, threat hunting, and continuous optimisation aligned with DigitalXRAID's SOC operations.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation
Service	Cyber Security as a Service (CSaaS)	Cyber Security as a Service (CSaaS) is an integrated, outsourced security model that combines managed detection, response, compliance, and consultancy services. It provides organisations with flexible, scalable cybersecurity capabilities without the cost and complexity of maintaining an in-house security team.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation

Service	Managed Vulnerability Scanning	Managed Vulnerability Scanning is a continuous vulnerability scanning service that identifies weaknesses across networks, systems, and applications. Regular reporting and risk-based prioritisation enable organisations to address critical vulnerabilities and reduce exposure to known threats efficiently.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation
Service	IT Health Check	IT Health Check is a comprehensive security testing service aligned with government and regulatory requirements. It identifies vulnerabilities across systems and networks, validates security controls, and provides actionable remediation guidance to strengthen overall security posture and support compliance obligations.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation
Service	Cyber Incident Exercising	Cyber Incident Exercising consists of simulated cyber-attack exercises designed to test incident response readiness. Table-top and scenario-based simulations validate processes, roles, and communications. These exercises help organisations refine response plans, improve decision-making, and enhance preparedness for real-world incidents.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation
Service	Cyber Security Maturity Assessment	The Cyber Security Maturity Assessment is a structured evaluation that assesses people, processes, and technology against recognized frameworks such as NIST. It identifies security gaps, measures current maturity levels, and delivers a prioritised roadmap to strengthen cyber resilience and align security strategy with business objectives.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech

			▪ Manufacturing ▪ Media ▪ Transportation
Service	ISO 27001 Certification	DigitalXRAID provides end-to-end ISO 27001 certification support, including gap analysis, risk assessment, ISMS design, implementation, and audit readiness. DigitalXRAID guides organisations through certification and ongoing maintenance to ensure continual compliance and improved information security governance.	▪ Education ▪ Technology ▪ Property ▪ Energy ▪ Finance ▪ Government ▪ Healthcare ▪ Fintech ▪ Manufacturing ▪ Media ▪ Transportation

Source: Company Website

5.1.3 RECENT DEVELOPMENTS

5.1.3.1 Product enhancements

TABLE 30 DIGITALXRAID: ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
March 2024	Product Enhancement	DigitalXRAID (UK)	Managed Security Operations Centre (SOC) (Service)	DigitalXRAID enhanced its Managed SOC service by integrating a more comprehensive dark web threat intelligence service through a partnership with Searchlight Cyber. This enhancement provides analysts with expanded visibility into hidden cybercriminal activity and external threat indicators, enabling earlier detection and more informed incident response.

Source: Company Website and Press Releases

5.1.3.2 Deals

TABLE 31 DIGITALXRAID: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
November 2024	Partnership	DigitalXRAID (UK)	Vanta (US)	DigitalXRAID partnered with Vanta to join its Managed Service Provider (MSP) program, integrating Vanta's trust management platform into DigitalXRAID's MSS offerings. This enables automated, continuous compliance monitoring, streamlined risk management, and the faster achievement of frameworks like ISO 27001 and SOC 2.

March 2024	Partnership	DigitalXRAID (UK)	Searchlight Cyber (UK)	DigitalXRAID partnered with Searchlight Cyber to enhance its Managed SOC service with comprehensive dark web intelligence. This integration enables analysts to detect threats proactively, improve incident response, and continuously monitor and mitigate emerging cyber threats.

Source: Company Website and Press Releases

5.1.3.3 Expansions

TABLE 32 DIGITALXRAID: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
July 2025	Expansion	MSS Service Scale via Group Formation	UK	DigitalXRAID (UK)	Through its acquisition by Limerston Capital, DigitalXRAID expanded its MSS and cyber capabilities as part of a wider group. The integration strengthened SOC, MDR, incident response, digital forensics, and consultancy services at scale.
March 2024	Expansion	Regional Business Growth	UK	DigitalXRAID (UK)	DigitalXRAID expanded its presence within the Liverpool business community by joining the Liverpool Chamber of Commerce. This move boosted regional engagement, strengthened visibility for its MSS expertise, and brought cybersecurity services closer to local businesses in the UK.
June 2023	Expansion	SOC & MSS Workforce Expansion	UK	DigitalXRAID (UK)	DigitalXRAID expanded its Security Operations Centre (SOC) and managed security workforce with significant hiring to support 24/7 threat protection and SOC service delivery. This expansion reflects strong demand from MSS clients and continued business growth.

Source: Company Website and Press Releases

6 APPENDIX

6.1 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL

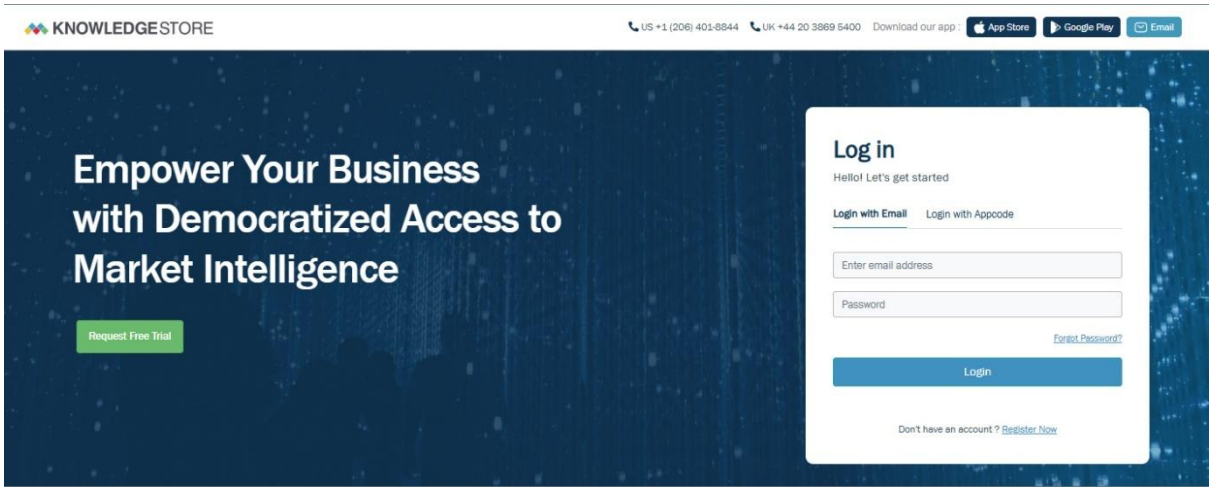
KnowledgeStore contains unique market insights from MarketsandMarkets. As a subscriber, you can access all published titles and any new ones added over the subscription period. You can subscribe to a specific number of reports or domains of your interest.

KNOWLEDGESTORE ENABLES YOU TO:

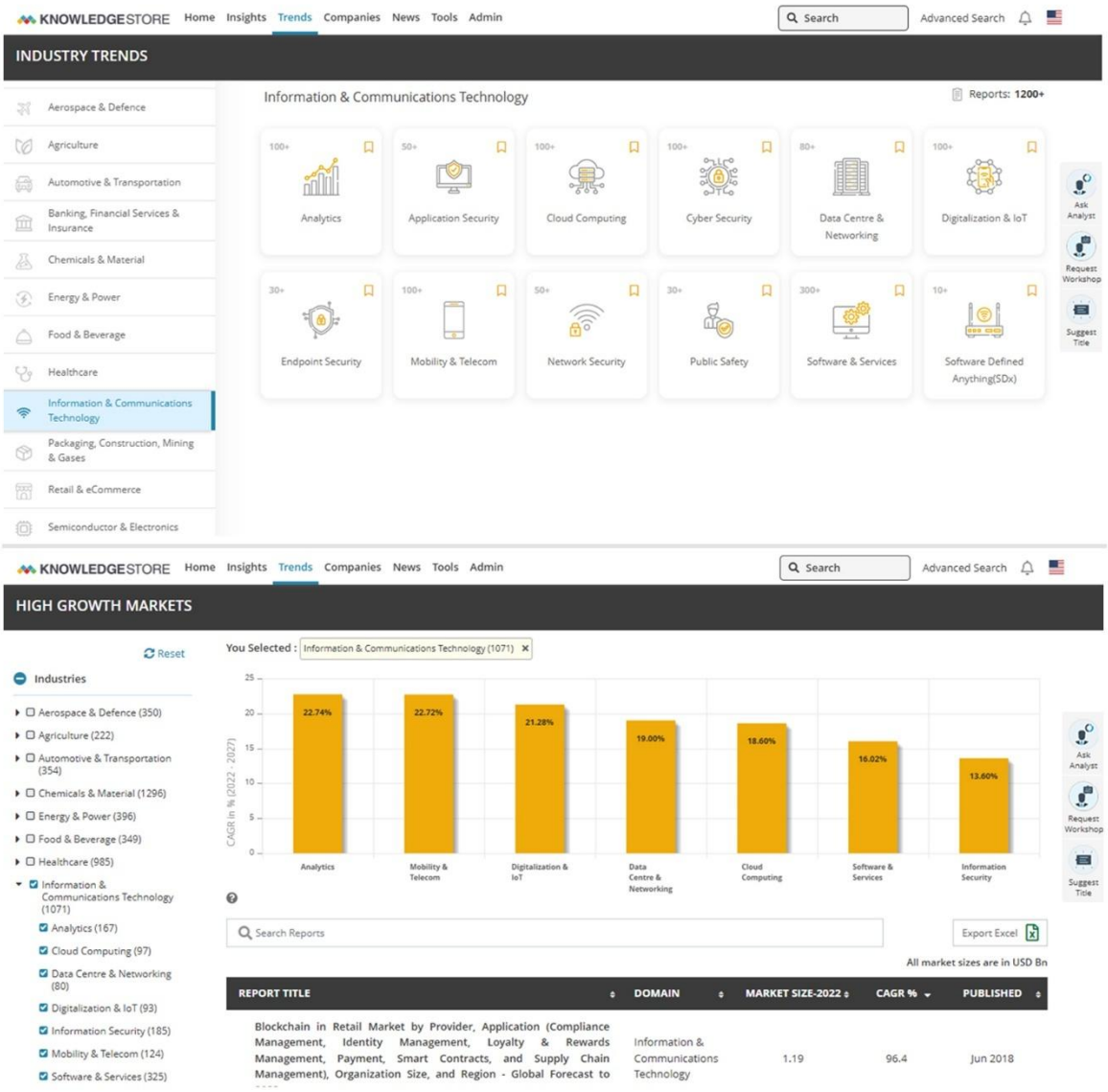
- View & download all subscribed reports from a single, online platform
- Contact our analysts to answer any questions related to our reports or request custom research
- Share comments on specific reports with the other users of your organization
- Suggest titles/topics to our research teams that you would like us to cover in our future reports
- Identify reports published on the high-growth markets within your industry

Get started now by requesting a demo and learning more about KnowledgeStore at www.mnmks.com.

MARKETSANDMARKETS KNOWLEDGESTORE SNAPSHOT



MARKETSANDMARKETS KNOWLEDGESTORE: INFORMATION & COMMUNICATION TECHNOLOGY SNAPSHOT



6.2 COMPANY EVALUATION MATRIX: METHODOLOGY

We evaluate, assess, and compare companies operating within this market on two key parameters:

- Market Share/Rank
- Product Footprint

A structured, data-driven approach is employed to ensure objective and consistent analysis across all companies and parameters. Each company is assessed using a predefined set of criteria tailored to each parameter. Market Share Rank measures a company's position in the market based on revenue, customer base, and overall sales volume, while Product Footprint evaluates the breadth and depth of the company's product offerings, including product variety, product features & functionality, product branding, technology footprint, end-use industries served and regional coverage. Our methodology follows a systematic data collection, validation, and comparative analysis process to ensure accuracy and reliability in ranking companies within the market landscape.

Companies are rated on the above parameters, and an overall score is assigned for each variable. The scores are a result of an in-depth quantitative and qualitative analysis of markets and a complete 360-degree view of competitors. Primary and secondary research plays a critical role in the overall data collection process, besides utilizing our in-house expertise and industry tracking methods. Executives of major industry participants across the value chain are also interviewed to acquire the most accurate and current data.

Quality control is a critical component of our research methodology and comprises several layers of checks by senior consultants and subject matter experts. These experts review the findings, ratings, and positioning of various players in the graph at different stages of the production cycle to ensure an authentic representation of companies on the graph.

An indicative list of questions considered to measure a player on each criterion is listed below.

MARKET SHARE/RANK

Revenue:

- What was the company's market share for the last year? Was this an increase/decrease over the previous year?
- What was the company's total revenue for the last three fiscal years?
- How does the company's pricing compare to other players in the market?
- What percentage of the company's revenue comes from products/services within the market versus other business lines?
- What was the company's average annual growth rate over the past three years?
- What growth strategies has the company adopted over the past three years?
- Does the company growth exceed the industry average? How does it compare to the growth of the competitors?

Customer Base:

- How many active customers does the company currently serve?
- What is the company's customer retention rate over the past three years?
- What percentage of the revenue comes from repeat customers versus new customers?
- What is the geographic distribution of the company's customer base?

Overall Sales Volume:

- What was the company's total sales volume (units sold or transactions completed) for the last fiscal year? Last 3 fiscal years?
- How does the company's sales volume vary across regions or customer segments?
- Does the company experience seasonal spikes or downturns in sales? If so, can the company scale up to meet the seasonal spike in demand successfully?
- What percentage of the company's total sales volume comes from new markets or recently launched products?

PRODUCT FOOTPRINT

Breadth and Depth of Products Offered:

- How wide and deep is the company's product line?
- Is the product line narrow, or too wide, or optimal?
- Is it wide enough to serve multiple applications or end-markets?
- Is it deep enough to provide various products at different price points and features in order to meet diverse customer needs?
- How many distinct products or services does the company currently offer?
- How frequently does the company launch new products or update existing ones? How many new products or services has the company launched in the last year?
- What percentage of the company's products/services are exclusive or unique compared to competitors?
- Does the company have exclusive patents, proprietary technology, or specialized expertise in its product offerings?

End-use Industries Served:

- What percentage of the company's revenue is generated from each industry segment?
- Does the company cater to all end-user segments? If not, how many end-use segments does the company offer its products/services in?

Technologies Covered:

- Which technologies does the company cater to? Are any technologies covered that competitors don't cover, or are exclusive to you? How do you compare to competitors in the market?
- What percentage of the company's revenue is allocated to research and development?
- Which emerging technologies are integrated into the company's product?
- How easy is updating or upgrading the company's product with new technology?
- How adaptable is the technology to emerging industry trends and regulatory changes?
- Does the company's products/services support sustainability and energy efficiency (where applicable)?

Regions Covered:

- In how many countries or regions are the company's products currently available?
- What are the key markets for the company's products?
- Has the company expanded into new markets in the last three years? If so, which ones?
- What percentage of the company's revenue comes from international markets?

Product Features and Functionality:

- What is the level of the company's focus on offering value-added features and functionality to its customers?
- What are the unique product/service features that differentiate it from competitors?
- How does the comprehensiveness of the company's product features/functionality compare to industry benchmarks or competitors?
- Are AI, automation, or smart features integrated into the company's product/service? If so, how do they enhance user experience?

Product Branding:

- Has the company received any industry awards, certifications, or media recognition?
- How often do customers mention the company's brand organically on social media or in reviews?

6.3 AUTHOR DETAILS

Vivek Ravichandran
Senior Research Manager, Information and Communications Technology

14+ years of experience in Business Advisory, Strategy & Growth Consulting, and Best Practices Benchmarking.

In his current role, Vivek focuses on revenue impact for clients through new revenue opportunities driven by the ever-changing revenue mix, use cases driving the change, and how clients can tap new revenue streams while leveraging the current revenue streams (cash cows).

Before MarketsandMarkets, he worked with Ramco Systems, Zinnov (deputed), Infiniti Research (TechNavio), and Cognizant, where he played the role of a strategic partner for Mobility and CIS teams to penetrate key accounts from core pillars and strengthen revenue streams.

Vivek holds a Master's in Business Administration from NMIMS with a dual specialization in Finance and Marketing and a Bachelor of Engineering in Electronics and Communication from Anna University.

Contributors

Sayali Saste
Associate Manager

Shivam Jethwa
Team Lead

Pratiksha Sonawane
Research Associate

Disclaimer: This document contains highly confidential information and is the sole property of 360Quadrants. The information provided herein is on an 'as is' and 'as available' basis and may not be circulated, copied, quoted, or otherwise reproduced or distributed in any form, including photocopying, mechanical, electronic, recording, or otherwise, without prior written permission from 360Quadrants. Under no circumstance shall 360Quadrants have any liability for any loss or damage of any kind incurred as a result of the use of the site or reliance on any information provided on the site. We disclaim all warranties of any kind, including but not limited to any express warranties, statutory warranties, and any implied warranties of merchantability, fitness for a particular purpose, and non-infringement. Your use of the site and your reliance on any information on the site is solely at your own risk. Views and opinions contained in testimonials belong solely to the individual user and do not reflect the views and opinions of 360Quadrants. 360Quadrants is not affiliated with users who provide testimonials, and users are not paid or otherwise compensated for their testimonials. Trademarks, copyrights, and other forms of intellectual property belong to 360Quadrants or their respective owners and are protected by law. Under no circumstance may any of these be reproduced, copied, or circulated in any form without the prior written approval of 360Quadrants or its owner—as the case may be.

Copyright © 2025 360Quadrants. All Rights Reserved.

For information regarding permission, contact:
Tel: +1-888-600-6441
support@360quadrants.com