Managed Security Services (MSSP) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 136 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

Managed Security Services (MSSP) Market Analysis

The managed security services market size stands at USD 38.31 billion in 2025 and is forecast to reach USD 69.16 billion by 2030 at a 12.54% CAGR. Heightened regulatory pressure, notably the European Union's DORA and NIS2 directives, drives enterprises to embed security controls at the design stage rather than bolting them on later. Organizations are moving from reactive defenses to AI-enabled, predictive threat detection that scales across hybrid environments. Accelerated cloud migration, widening multi-cloud attack surfaces and an intensifying cyber-talent shortage further enlarge outsourcing demand. Competition is intensifying as cloud hyperscalers integrate security analytics into their platforms, forcing traditional providers to differentiate through vertical expertise and unified security architectures. Consolidation continues, with 2024's USD 859 million Sophos-Secureworks deal showing providers' urgency to acquire advanced analytics capabilities.

Global Managed Security Services (MSSP) Market Trends and Insights

AI-led SOC automation and XDR adoption surge

Organizations are embedding artificial intelligence into security operations centers to shorten detection and response cycles and limit analyst fatigue. Microsoft's Security Copilot integrated with Defender XDR cuts mean time to respond by 40% and slashes false positives by 60%, showcasing how generative AI speeds triage and improves fidelity. Palo Alto Networks' Cortex XSIAM already processes 1 trillion daily events to surface hidden attack paths, enabling MSSPs to deliver outcome-based SLAs that justify

premium pricing.The approach also mitigates talent shortages, allowing 24/7 monitoring with smaller analyst teams. As AI-native competitors proliferate, traditional providers risk margin compression unless they embed autonomous investigation and response at scale. Over the medium term, successful MSSPs will fuse AI models with proprietary threat intelligence to anticipate attacks before initial compromise.

Escalating multi-cloud attack surface

Wide adoption of AWS, Azure and Google Cloud creates fragmented visibility, leaving security gaps that hackers exploit. CrowdStrike recorded a 75% year-over-year rise in cloud intrusions during 2024, driven by misconfigurations and over-privileged identities. Enterprises now juggle 3.2 security integrations per cloud, compounding alert noise. Google Cloud's SecOps platform crunches 400 billion signals each day, illustrating the analytic horsepower needed to filter genuine threats. MSSPs able to ingest telemetry from multiple clouds into a single analytics fabric gain share by simplifying operations and cutting tool overheads. In the short term, demand for cloud-native threat monitoring outpaces supply of qualified experts, fueling double-digit growth across the managed security services market.

Persistent trust deficit in data-sovereignty

European clients balk at shipping telemetry to SOCs outside EU borders even when providers boast GDPR clauses. India, China and Brazil enforce localization statutes that fragment global delivery models, raising provider overheads. The 2025 Marks & Spencer breach, traced back to a third-party vendor, cost EUR 300 million in lost sales and amplified concerns over extended supply chains. To win contracts, MSSPs add domestic SOC footprints and guarantee residency for sensitive logs, but duplicating infrastructure erodes margins. Over the next three years, data-sovereignty constraints temper growth in heavily regulated verticals even as demand rises.

Other drivers and restraints analyzed in the detailed report include:

Compliance-by-design mandates (DORA, NIS2, SEC) / Cost and talent crunch pushing co-managed MSS / Tool sprawl and integration complexity /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Cloud-based services accounted for 72.3% of the managed security services market in 2024 as enterprises re-platformed security controls alongside workloads. The segment is forecast to expand at a 14.7% CAGR through 2030, reflecting confidence in hyperscaler resilience and AI-infused analytics. Providers operate global PoPs that ingest logs at petabyte scale, then apply machine learning to spot lateral movement within minutes. Cost benefits compound adoption: CIOs report 45% lower total cost of ownership and 60% faster time-to-value compared with appliance-centric deployments. On-premises models persist in defense and highly classified environments where air-gap mandates override scalability concerns. Hybrid approaches emerge, with sensitive logs stored locally while non-classified telemetry streams to cloud SIEMs for aggregated analytics. The managed security services market size for cloud deployments is poised to widen its lead as 5G and edge compute push telemetry volumes higher. Meanwhile, providers redesign SLAs around latency and uptime guarantees to reassure regulated customers.

Second-generation cloud architectures emphasize API-level integration rather than lift-and-shift virtual appliances. Zscaler's alliance with BT illustrates the model: BT funnels 400 billion daily sessions through Zscaler's cloud to gain real-time risk scoring on every transaction. Such scale delivers threat intelligence inaccessible to siloed deployments, creating a feedback loop that continuously improves detection. Geopolitical tensions, however, force hyperscalers to build sovereign clouds, which may dilute

centralization benefits. Nonetheless, with SaaS adoption in double digits, the managed security services market continues to pivot decisively toward cloud-first delivery.

Managed Detection and Response held 27.3% of the managed security services market share in 2024, posting a 12.9% CAGR as customers demand active containment rather than ticket-only monitoring. MDR fuses endpoint telemetry, network flow data and identity context to surface anomalous behavior. Providers couple 24/7 analyst eyes with automated response playbooks, isolating patient-zero hosts in seconds. Traditional firewall management faces commoditization, but remains necessary for compliance-driven perimeter controls. Identity-centric zero-trust services are rising, particularly among SaaS-heavy mid-size enterprises.

AI-enabled MDR platforms such as Red Canary's Managed XSIAM harness log-correlation engines to cut dwell time and shrink breach impact. Increased pairing of MDR with vulnerability management supports continuous remediation loops. DDoS mitigation stays relevant for uptime assurance, while managed IAM services close privilege-escalation gaps. Overall, layered MDR bundles position providers as strategic partners, underpinning sticky three- to five-year contracts that swell the managed security services market size for outcome-focused offerings.

Managed Security Services (MSSP) Market is Segmented by Deployment Model (On-Premises, Cloud), Service Type (Managed Detection and Response (MDR), Firewall and UTM Management, Intrusion Detection/Prevention, and More), Provider Type (IT Service Integrators, Security-Specialist MSSPs, and More), End-User Industry (BFSI, Government and Defense, and More), and by Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America held 29.3% of global revenue in 2024, buoyed by stringent SEC disclosure rules and ready access to venture funding that fuels security innovation. US firms lead adoption of AI-driven SOCs and quantum-resistant pilots, whereas Canadian utilities focus on critical-infrastructure hardening aligned with C-SCRM guidance. Mexico's automotive corridor embraces co-managed SOCs to offset talent deficits. Despite saturation at large enterprises, mid-market penetration remains underscored by ransomware's financial impact, sustaining double-digit spend.

Asia-Pacific is growing fastest at 13.1% CAGR through 2030. Japan's manufacturers fortify OT assets after multiple supply-chain breaches; China emphasizes domestically developed SOC platforms under data-localization mandates; India's small and mid-size firms outsource log monitoring to bridge skills shortfalls. ASEAN banks face digital-payments fraud surges, prodding regulators to raise breach-reporting fines that boost managed security services market demand. South Korea pioneers 5G-edge protection frameworks, positioning local MSSPs as exporters of MEC-centric threat analytics.

Europe advances steadily due to DORA and NIS2. Germany invests in industrial-control defenses, the UK emphasizes financial-sector resilience post-Brexit, and France nurtures sovereign-cloud SOCs. Mediterranean SMEs turn to MDR subscriptions to meet insurance prerequisites. Data-residency stipulations favor regional SOC buildouts, compelling global providers to partner with domestic data-center operators. Collectively, regulatory harmonization and funding initiatives anchor a compliance-driven managed security services market across the continent.

List of Companies Covered in this Report:

AT&T / IBM / Secureworks / Verizon / Broadcom (Symantec) / Atos / Lumen Technologies / BAE Systems / Capgemini / Fujitsu / Wipro / Trustwave / Fortra / Deloitte / NTT / Accenture / Palo Alto Networks / BT Group / Orange Cyberdefense / Kyndryl /

Additional Benefits:

 The market estimate (ME) sheet in Excel format /
 3 months of analyst support /

Table of Contents:

5.5.5.2.1 South Africa
5.5.5.2.2 Nigeria
5.5.5.2.3 Egypt
5.5.5.2.4 Rest of Africa

6 COMPETITIVE LANDSCAPE
6.1 Market Concentration
6.2 Strategic Moves
6.3 Market Share Analysis
6.4 Company Profiles (includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share for key companies, Products and Services, and Recent Developments)
6.4.1 AT&T
6.4.2 IBM
6.4.3 Secureworks
6.4.4 Verizon
6.4.5 Broadcom (Symantec)
6.4.6 Atos
6.4.7 Lumen Technologies
6.4.8 BAE Systems
6.4.9 Capgemini
6.4.10 Fujitsu
6.4.11 Wipro
6.4.12 Trustwave
6.4.13 Fortra
6.4.14 Deloitte
6.4.15 NTT
6.4.16 Accenture
6.4.17 Palo Alto Networks
6.4.18 BT Group
6.4.19 Orange Cyberdefense
6.4.20 Kyndryl

7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK
7.1 White-space and Unmet-need Assessment

Managed Security Services (MSSP) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 136 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-03
		Signature