+357 96 030922
info@marketpublishers.com

Managed Security Services Market Forecasts to 2034 – Global Analysis By Service Type (Managed Detection and Response (MDR), Managed Identity and Access Management (IAM), Managed Firewall, Managed Intrusion Detection and Prevention Systems (IDPS), Managed Endpoint Security, Managed Vulnerability Management, Managed Security Information and Event Management (SIEM), Managed Risk & Compliance, and Other Service Types), Deployment Mode, Organization Size, Security Type, End User, Enterprise Type, and By Geography

https://marketpublishers.com/r/MC8580E62547EN.html
Date: July 2026
Pages: 0
Price: US$ 4,150.00 (Single User License)
ID: MC8580E62547EN

Abstracts

According to Stratistics MRC, the Global Managed Security Services Market is accounted for $42.4 billion in 2026 and is expected to reach $109.7 billion by 2034 growing at a CAGR of 12.6% during the forecast period. Managed Security Services refer to outsourced monitoring and management of security devices, systems, and procedures by specialized third-party providers. These services include managed detection and response, managed identity and access management, managed firewall, managed intrusion detection and prevention systems, managed endpoint security, managed vulnerability management, managed security information and event management, managed risk and compliance, and other security services. The market serves organizations across all industries, deployed through on-premise, cloud, and hybrid models. Rising cybersecurity threats, increasing regulatory compliance requirements, and the growing complexity of security environments are key drivers of market expansion.

+357 96 030922
info@marketpublishers.com

Market Dynamics:

Driver:

Escalating cybersecurity threats and sophistication of attacks

The rapid increase in cyberattacks and growing sophistication of threat actors are primary drivers for the managed security services market. Organizations face evolving threats including ransomware, phishing, advanced persistent threats, and zero-day exploits that require continuous monitoring and rapid response. The proliferation of connected devices and expanding attack surfaces create additional vulnerabilities. Security skills shortages limit many organizations' ability to maintain effective in-house security operations, driving outsourcing to specialized providers. Managed security services offer 24/7 monitoring, threat intelligence integration, and access to skilled security professionals that most organizations cannot afford internally. As cyber threats continue escalating, demand for managed security services continues growing across all industry verticals.

Restraint:

Concerns about data privacy and vendor lock-in

Data privacy concerns and potential vendor lock-in represent significant restraints for the managed security services market. Organizations must share sensitive information about their networks, systems, and vulnerabilities with external providers, raising concerns about data confidentiality. Regulatory requirements including GDPR and industry regulations impose strict obligations on data processing, requiring careful vendor selection and contract negotiation. Switching between managed security service providers can be complex and costly, creating dependency concerns. Organizations may hesitate to outsource security functions critical to business operations. These concerns may slow adoption among risk-averse organizations, particularly in highly regulated industries.

Opportunity:

Integration of AI and automation in security operations

The integration of artificial intelligence and automation with managed security services presents significant opportunities for market expansion. AI-powered security tools enable faster threat detection, automated incident response, and reduced false positives. Machine learning algorithms analyze security data to identify patterns and predict potential attacks. Automated playbooks enable rapid response to common threats, reducing manual intervention. Security orchestration, automation, and response (SOAR) platforms streamline operations and improve efficiency. As AI capabilities continue advancing, managed security services become more effective and cost-efficient, attracting organizations seeking enhanced protection without proportional cost increases.

Threat:

Competition from in-house security teams and technology vendors

Competition from internal security operations and technology vendors offering integrated security capabilities poses significant threats to the managed security services market. Large enterprises may develop in-house security operations centers with advanced capabilities, reducing outsourcing needs. Cloud providers are expanding their native security services, including threat detection and compliance monitoring. Security technology vendors are offering managed services components alongside their products. Organizations may choose to retain certain security functions internally while outsourcing others, creating competitive dynamics. This competition may limit market growth in certain segments and regions.

Covid-19 Impact:

The COVID-19 pandemic significantly accelerated managed security services adoption as organizations rapidly shifted to remote work and expanded digital operations. The sudden expansion of attack surfaces through remote access and cloud services created immediate security needs that many organizations could not meet internally. Managed security providers enabled rapid deployment of security monitoring and response capabilities. Supply chain security concerns and increased cyber threats including pandemic-related phishing campaigns drove demand. Post-pandemic, hybrid work models have sustained elevated demand for managed security services, with organizations maintaining or expanding outsourced security capabilities. The crisis permanently raised awareness of security vulnerabilities and the value of specialized services.

The Managed Detection and Response (MDR) segment is expected to be the largest during the forecast period

The Managed Detection and Response (MDR) segment is expected to account for the largest market share during the forecast period, driven by increasing demand for proactive threat hunting, rapid incident response, and continuous security monitoring. MDR services provide organizations with 24/7 threat detection, investigation, and response capabilities that many lack internally. The segment benefits from growing sophistication of threats, rising security skills shortages, and the increasing complexity of security environments. MDR providers combine advanced technology, threat intelligence, and security expertise to deliver comprehensive protection. As organizations prioritize detection and response capabilities to address evolving threats, MDR maintains the largest service type market share throughout the forecast period.

The Cloud segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the Cloud segment is predicted to witness the highest growth rate, fueled by the rapid migration of workloads and security operations to cloud environments. Cloud-based managed security services offer advantages including scalability, rapid deployment, automatic updates, and reduced infrastructure costs. Organizations increasingly prefer cloud delivery for its flexibility and integration with cloud-native applications and workloads. Remote security management is facilitated through cloud-based platforms. Security providers are investing in cloud-native architectures to improve performance and reduce costs. As cloud adoption continues accelerating across all industries, cloud-based managed security services deliver the fastest segment growth.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, supported by high cybersecurity awareness, strong regulatory compliance requirements, and the presence of major managed security service providers. The United States leads global security spending, with organizations across all sectors investing in robust protection. Strict regulatory frameworks including HIPAA, PCI DSS, and state privacy laws drive service adoption. The region's large enterprise base with sophisticated security needs creates substantial demand. Continuous innovation and vendor presence support market growth. With strong security culture and investment, North America maintains its dominant market position.

Region with highest CAGR:

Over the forecast period, the Asia-Pacific region is anticipated to exhibit the highest CAGR, driven by rapid digital transformation, increasing cyber threats, and growing regulatory requirements across countries including China, India, Australia, and Singapore. The region's expanding technology adoption and digital economy create growing security needs. Rising awareness of cybersecurity threats and importance of protection drives service adoption. Government cybersecurity initiatives and regulations are increasing compliance requirements. Growing enterprise investment in security supports market expansion. As digital transformation accelerates and security becomes a priority, Asia Pacific delivers the fastest managed security services market growth globally.

Key players in the market

Some of the key players in Managed Security Services Market include IBM Corporation, Cisco Systems, Inc., AT&T Inc., Verizon Communications Inc., Broadcom Inc., Fortinet, Inc., Check Point Software Technologies Ltd., Palo Alto Networks, Inc., Trustwave Holdings, Inc., Secureworks Inc., Wipro Limited, Tata Consultancy Services Limited, Accenture plc, Infosys Limited, Fujitsu Limited, NTT DATA Group Corporation, DXC Technology Company, and Hewlett Packard Enterprise Development LP.

Key Developments:

In July 2026, Lumen Technologies expanded its Defender Advanced Managed Detection and Response (AMDR) offering by integrating Palo Alto Networks' Cortex XSIAM platform with Black Lotus Labs threat intelligence to automate SOC operations.

In June 2026, ServiceNow and Accenture launched joint AI-powered managed security services built on the ServiceNow AI Platform, utilizing autonomous agentic workflows to unify IT and OT risk monitoring.

In June 2026, LTIMindtree (LTM) launched its Managed Secure Service Edge (SSE) solution powered by Cisco Secure Access at Cisco Live 2026, delivering 24/7 AI-driven managed threat detection across hybrid architectures.

In March 2026, Cisco integrated Splunk security analytics directly into its core data center network management stack, allowing MSS partners to automate root-cause analysis and incident remediation.

Service Types Covered:

- Managed Detection and Response (MDR)
- Managed Identity and Access Management (IAM)
- Managed Firewall
- Managed Intrusion Detection and Prevention Systems (IDPS)
- Managed Endpoint Security
- Managed Vulnerability Management
- Managed Security Information and Event Management (SIEM)
- Managed Risk and Compliance
- Other Service Types

Deployment Modes Covered:

- On-Premise
- Cloud
- Hybrid

Organization Sizes Covered:

- Small and Medium-Sized Enterprises (SMEs)
- Large Enterprises

Security Types Covered:

Network Security

Endpoint Security

Cloud Security

Application Security

Data Security

Identity and Access Security

End Users Covered:

BFSI

IT and Telecom

Healthcare

Retail and E-commerce

Government and Defense

Manufacturing

Energy and Utilities

Education

Media and Entertainment

Other End Users

Enterprise Types Covered:

Enterprises

+357 96 030922
info@marketpublishers.com

Small and Medium Enterprises

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Thailand

Malaysia

Singapore

Vietnam

Rest of Asia Pacific

South America

Brazil

Argentina

Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of Africa

What our report offers:

Market share assessments for the regional and country-level segments

Strategic recommendations for the new entrants

Covers Market data for the years 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034

Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)

Strategic recommendations in key business segments based on the market estimations

Competitive landscaping mapping the key common trends

Company profiling with detailed strategies, financials, and recent developments

Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

14 COMPANY PROFILES

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

Table 38 Global Managed Security Services Market Outlook, By Enterprises (2023-2034) ($MN)
Table 39 Global Managed Security Services Market Outlook, By Small and Medium Enterprises (2023-2034) ($MN)
Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Managed Security Services Market Forecasts to 2034 – Global Analysis By Service Type (Managed Detection and Response (MDR), Managed Identity and Access Management (IAM), Managed Firewall, Managed Intrusion Detection and Prevention Systems (IDPS), Managed Endpoint Security, Managed Vulnerability Management, Managed Security Information and Event Management (SIEM), Managed Risk & Compliance, and Other Service Types), Deployment Mode, Organization Size, Security Type, End User, Enterprise Type, and By Geography

Product link: https://marketpublishers.com/r/MC8580E62547EN.html

Price: US$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/MC8580E62547EN.html