

Attack Surface Management (ASM) Market Forecasts to 2034 – Global Analysis By Offering (Software/Platform and Services), Deployment Mode, Asset Type, Attack Surface Type, Application, End User and By Geography

<https://marketpublishers.com/r/AF82B40D1103EN.html>

Date: August 2026

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: AF82B40D1103EN

Abstracts

According to Statistics MRC, the Global Attack Surface Management (ASM) Market is accounted for \$1.4 billion in 2026 and is expected to reach \$8.9 billion by 2034, growing at a CAGR of 25.8% during the forecast period. Attack Surface Management is a comprehensive security solution that provides organizations with continuous discovery, monitoring, and assessment of all external and internal assets, including web applications, APIs, domains, cloud resources, endpoints, IoT devices, and identity infrastructure. ASM solutions aggregate data from diverse sources to create a unified view of the entire attack surface, enabling security teams to identify vulnerabilities, misconfigurations, and exposure risks across hybrid and multi-cloud environments. This technology helps organizations reduce security blind spots, prioritize remediation efforts, and proactively manage their attack surface.

Market Dynamics:

Driver:

Growing digital transformation and expanding attack surface

The accelerating pace of digital transformation and the corresponding expansion of organizational attack surfaces serve as primary drivers for the Attack Surface Management market. Organizations are rapidly adopting cloud services, APIs, microservices, and IoT devices, creating an increasingly complex and distributed attack

surface. Traditional asset discovery approaches are insufficient for modern dynamic environments, creating security blind spots that attackers exploit. ASM solutions provide continuous, automated discovery and monitoring of all assets, enabling organizations to identify and remediate exposures before they can be exploited. As digital transformation accelerates, the demand for comprehensive attack surface management solutions continues to grow significantly.

Restraint:

Integration complexity and data normalization challenges

The significant integration complexity and data normalization challenges pose restraints to the Attack Surface Management market. Organizations operate heterogeneous security tool ecosystems with varying data formats, APIs, and coverage. Aggregating and normalizing data from disparate sources across internal and external environments requires substantial engineering effort and ongoing maintenance. Ensuring data accuracy and eliminating duplicates across multiple data sources adds complexity. These integration challenges can slow adoption and increase implementation costs.

Opportunity:

AI-powered risk prioritization and predictive exposure analytics

The integration of AI-powered risk prioritization and predictive exposure analytics presents significant opportunities for the Attack Surface Management market. Machine learning algorithms can analyze asset criticality, vulnerability severity, threat intelligence, and exploitability to prioritize remediation efforts based on business impact. Predictive analytics can forecast emerging risks, identify attack paths, and recommend proactive security controls. As organizations seek to reduce risk exposure and optimize security investments, the demand for intelligent ASM solutions continues to grow.

Threat:

Competition from integrated security platforms

Competition from integrated security platforms poses significant threats to the Attack Surface Management market. Major security vendors are incorporating attack surface discovery and monitoring capabilities into their broader platforms, potentially reducing the need for standalone ASM solutions. The integration of ASM features into

comprehensive security platforms offers simplified architecture and reduced operational overhead. This competitive dynamic can pressure standalone ASM vendors to differentiate through specialized capabilities and deep integration with security ecosystems.

Covid-19 Impact:

The COVID-19 pandemic dramatically accelerated the adoption of Attack Surface Management solutions as organizations rapidly expanded remote workforces and cloud infrastructure, creating unprecedented asset visibility challenges. The sudden shift to distributed environments left many organizations with incomplete asset inventories and security blind spots. ASM platforms helped organizations discover previously unknown assets, identify security gaps, and prioritize remediation efforts. The crisis highlighted the critical importance of continuous asset visibility for maintaining security posture in dynamic environments, permanently expanding the market for attack surface management solutions.

The software/platform segment is expected to be the largest during the forecast period

The software/platform segment is expected to account for the largest market share during the forecast period, driven by the fundamental need for the core ASM platform that provides asset discovery, continuous monitoring, and risk visualization capabilities across external and internal environments. Organizations require comprehensive software platforms to discover and assess assets, identify vulnerabilities, and prioritize remediation efforts. The increasing complexity of hybrid environments drives investment in ASM software. Vendors offering integrated platforms with automated discovery, risk scoring, and threat intelligence integration are poised to capture significant market share.

The cloud-based segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the cloud-based segment is predicted to witness the highest growth rate, due to the scalability, flexibility, and ease of deployment of cloud-native ASM solutions. Cloud-based ASM enables organizations to discover and monitor assets across distributed environments without deploying on-premises infrastructure. The cloud delivery model supports rapid updates and integration with cloud-native security tools. As organizations embrace hybrid and multi-cloud environments, the demand for cloud-native ASM solutions continues to accelerate.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, driven by substantial cybersecurity spending, early adoption of attack surface management technologies, and the presence of major ASM providers. The region's focus on proactive security and asset visibility creates demand for comprehensive ASM solutions. Strong adoption across technology, financial services, and government sectors, where asset management is critical, contributes to market leadership.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, fueled by rapid digital transformation, expanding cloud adoption, and growing awareness of attack surface management across major economies. Countries such as China, India, and Australia are witnessing significant growth in ASM adoption as organizations modernize security operations. Rising cloud adoption, regulatory requirements, and the need to manage expanding attack surfaces position APAC as a key growth driver for the ASM market.

Key players in the market

Some of the key players in the Attack Surface Management (ASM) Market include Palo Alto Networks Inc., CrowdStrike Holdings Inc., Microsoft Corporation, Tenable Holdings Inc., Rapid7 Inc., Qualys Inc., Censys Inc., CyCognito Inc., IBM Corporation, Google LLC, Wiz Inc., Mandiant Inc., RiskIQ Inc., Detectify AB, and IONIX Inc.

Key Developments:

In June 2026, Palo Alto Networks announced significant enhancements to its attack surface management platform, including new external asset discovery capabilities and improved threat intelligence integration. The enhancements provide organizations with comprehensive visibility across their entire attack surface.

In May 2026, CrowdStrike introduced new ASM capabilities for cloud-native environments and third-party risk assessment. The enhancements enable organizations to discover and secure assets across hybrid and multi-cloud deployments.

Offerings Covered:

Software / Platform

Services

Deployment Modes Covered:

Cloud-Based

On-Premises

Hybrid

Asset Types Covered:

Web Applications

APIs

Domains & DNS Assets

IP Addresses & Network Infrastructure

Cloud Assets

Endpoints

IoT & OT Assets

Identity & Access Assets

Attack Surface Types Covered:

External Attack Surface Management (EASM)

Internal Attack Surface Management (IASM)

Cyber Asset Attack Surface Management (CAASM)

Cloud Attack Surface Management (CASM)

Third-Party / Supply Chain Attack Surface Management

Applications Covered:

Asset Discovery & Inventory

Continuous Monitoring

Vulnerability Identification

Risk Prioritization

Exposure Assessment

Threat Intelligence Integration

Compliance & Governance

Incident Response Support

End Users Covered:

BFSI

Government & Defense

Healthcare & Life Sciences

IT & Telecommunications

Manufacturing

Retail & E-commerce

Energy & Utilities

Media & Entertainment

Education

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

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL ATTACK SURFACE MANAGEMENT (ASM) MARKET, BY OFFERING

- 5.1 Software / Platform
- 5.2 Services
 - 5.2.1 Professional Services
 - 5.2.1.1 Consulting
 - 5.2.1.2 Implementation & Integration
 - 5.2.1.3 Training & Support
 - 5.2.2 Managed Services

6 GLOBAL ATTACK SURFACE MANAGEMENT (ASM) MARKET, BY DEPLOYMENT MODE

- 6.1 Cloud-Based
- 6.2 On-Premises
- 6.3 Hybrid

7 GLOBAL ATTACK SURFACE MANAGEMENT (ASM) MARKET, BY ASSET TYPE

- 7.1 Web Applications
- 7.2 APIs
- 7.3 Domains & DNS Assets
- 7.4 IP Addresses & Network Infrastructure
- 7.5 Cloud Assets
- 7.6 Endpoints
- 7.7 IoT & OT Assets
- 7.8 Identity & Access Assets

8 GLOBAL ATTACK SURFACE MANAGEMENT (ASM) MARKET, BY ATTACK SURFACE TYPE

- 8.1 External Attack Surface Management (EASM)
- 8.2 Internal Attack Surface Management (IASM)
- 8.3 Cyber Asset Attack Surface Management (CAASM)
- 8.4 Cloud Attack Surface Management (CASM)

8.5 Third-Party / Supply Chain Attack Surface Management

9 GLOBAL ATTACK SURFACE MANAGEMENT (ASM) MARKET, BY APPLICATION

- 9.1 Asset Discovery & Inventory
- 9.2 Continuous Monitoring
- 9.3 Vulnerability Identification
- 9.4 Risk Prioritization
- 9.5 Exposure Assessment
- 9.6 Threat Intelligence Integration
- 9.7 Compliance & Governance
- 9.8 Incident Response Support

10 GLOBAL ATTACK SURFACE MANAGEMENT (ASM) MARKET, BY END USER

- 10.1 BFSI
- 10.2 Government & Defense
- 10.3 Healthcare & Life Sciences
- 10.4 IT & Telecommunications
- 10.5 Manufacturing
- 10.6 Retail & E-commerce
- 10.7 Energy & Utilities
- 10.8 Media & Entertainment
- 10.9 Education

11 GLOBAL ATTACK SURFACE MANAGEMENT (ASM) MARKET, BY GEOGRAPHY

- 11.1 North America
 - 11.1.1 United States
 - 11.1.2 Canada
 - 11.1.3 Mexico
- 11.2 Europe
 - 11.2.1 United Kingdom
 - 11.2.2 Germany
 - 11.2.3 France
 - 11.2.4 Italy
 - 11.2.5 Spain
 - 11.2.6 Netherlands

- 11.2.7 Belgium
- 11.2.8 Sweden
- 11.2.9 Switzerland
- 11.2.10 Poland
- 11.2.11 Rest of Europe
- 11.3 Asia Pacific
 - 11.3.1 China
 - 11.3.2 Japan
 - 11.3.3 India
 - 11.3.4 South Korea
 - 11.3.5 Australia
 - 11.3.6 Indonesia
 - 11.3.7 Thailand
 - 11.3.8 Malaysia
 - 11.3.9 Singapore
 - 11.3.10 Vietnam
 - 11.3.11 Rest of Asia Pacific
- 11.4 South America
 - 11.4.1 Brazil
 - 11.4.2 Argentina
 - 11.4.3 Colombia
 - 11.4.4 Chile
 - 11.4.5 Peru
 - 11.4.6 Rest of South America
- 11.5 Rest of the World (RoW)
 - 11.5.1 Middle East
 - 11.5.1.1 Saudi Arabia
 - 11.5.1.2 United Arab Emirates
 - 11.5.1.3 Qatar
 - 11.5.1.4 Israel
 - 11.5.1.5 Rest of Middle East
 - 11.5.2 Africa
 - 11.5.2.1 South Africa
 - 11.5.2.2 Egypt
 - 11.5.2.3 Morocco
 - 11.5.2.4 Rest of Africa

12 STRATEGIC MARKET INTELLIGENCE

- 12.1 Industry Value Network and Supply Chain Assessment
- 12.2 White-Space and Opportunity Mapping
- 12.3 Product Evolution and Market Life Cycle Analysis
- 12.4 Channel, Distributor, and Go-to-Market Assessment

13 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

- 13.1 Mergers and Acquisitions
- 13.2 Partnerships, Alliances, and Joint Ventures
- 13.3 New Product Launches and Certifications
- 13.4 Capacity Expansion and Investments
- 13.5 Other Strategic Initiatives

14 COMPANY PROFILES

- 14.1 Palo Alto Networks
- 14.2 CrowdStrike
- 14.3 Microsoft
- 14.4 Tenable
- 14.5 Rapid7
- 14.6 Qualys
- 14.7 Censys
- 14.8 CyCognito
- 14.9 IBM
- 14.10 Google
- 14.11 Wiz
- 14.12 Mandiant
- 14.13 RiskIQ
- 14.14 Detectify
- 14.15 IONIX

List Of Tables

LIST OF TABLES

Table 1 Global Attack Surface Management (ASM) Market Outlook, By Region (2023-2034) (\$MN)

Table 2 Global Attack Surface Management (ASM) Market Outlook, By Offering (2023-2034) (\$MN)

Table 3 Global Attack Surface Management (ASM) Market Outlook, By Software / Platform (2023-2034) (\$MN)

Table 4 Global Attack Surface Management (ASM) Market Outlook, By Services (2023-2034) (\$MN)

Table 5 Global Attack Surface Management (ASM) Market Outlook, By Professional Services (2023-2034) (\$MN)

Table 6 Global Attack Surface Management (ASM) Market Outlook, By Consulting (2023-2034) (\$MN)

Table 7 Global Attack Surface Management (ASM) Market Outlook, By Implementation & Integration (2023-2034) (\$MN)

Table 8 Global Attack Surface Management (ASM) Market Outlook, By Training & Support (2023-2034) (\$MN)

Table 9 Global Attack Surface Management (ASM) Market Outlook, By Managed Services (2023-2034) (\$MN)

Table 10 Global Attack Surface Management (ASM) Market Outlook, By Deployment Mode (2023-2034) (\$MN)

Table 11 Global Attack Surface Management (ASM) Market Outlook, By Cloud-Based (2023-2034) (\$MN)

Table 12 Global Attack Surface Management (ASM) Market Outlook, By On-Premises (2023-2034) (\$MN)

Table 13 Global Attack Surface Management (ASM) Market Outlook, By Hybrid (2023-2034) (\$MN)

Table 14 Global Attack Surface Management (ASM) Market Outlook, By Asset Type (2023-2034) (\$MN)

Table 15 Global Attack Surface Management (ASM) Market Outlook, By Web Applications (2023-2034) (\$MN)

Table 16 Global Attack Surface Management (ASM) Market Outlook, By APIs (2023-2034) (\$MN)

Table 17 Global Attack Surface Management (ASM) Market Outlook, By Domains & DNS Assets (2023-2034) (\$MN)

Table 18 Global Attack Surface Management (ASM) Market Outlook, By IP Addresses

& Network Infrastructure (2023-2034) (\$MN)

Table 19 Global Attack Surface Management (ASM) Market Outlook, By Cloud Assets (2023-2034) (\$MN)

Table 20 Global Attack Surface Management (ASM) Market Outlook, By Endpoints (2023-2034) (\$MN)

Table 21 Global Attack Surface Management (ASM) Market Outlook, By IoT & OT Assets (2023-2034) (\$MN)

Table 22 Global Attack Surface Management (ASM) Market Outlook, By Identity & Access Assets (2023-2034) (\$MN)

Table 23 Global Attack Surface Management (ASM) Market Outlook, By Attack Surface Type (2023-2034) (\$MN)

Table 24 Global Attack Surface Management (ASM) Market Outlook, By External Attack Surface Management (EASM) (2023-2034) (\$MN)

Table 25 Global Attack Surface Management (ASM) Market Outlook, By Internal Attack Surface Management (IASM) (2023-2034) (\$MN)

Table 26 Global Attack Surface Management (ASM) Market Outlook, By Cyber Asset Attack Surface Management (CAASM) (2023-2034) (\$MN)

Table 27 Global Attack Surface Management (ASM) Market Outlook, By Cloud Attack Surface Management (CASM) (2023-2034) (\$MN)

Table 28 Global Attack Surface Management (ASM) Market Outlook, By Third-Party / Supply Chain Attack Surface Management (2023-2034) (\$MN)

Table 29 Global Attack Surface Management (ASM) Market Outlook, By Application (2023-2034) (\$MN)

Table 30 Global Attack Surface Management (ASM) Market Outlook, By Asset Discovery & Inventory (2023-2034) (\$MN)

Table 31 Global Attack Surface Management (ASM) Market Outlook, By Continuous Monitoring (2023-2034) (\$MN)

Table 32 Global Attack Surface Management (ASM) Market Outlook, By Vulnerability Identification (2023-2034) (\$MN)

Table 33 Global Attack Surface Management (ASM) Market Outlook, By Risk Prioritization (2023-2034) (\$MN)

Table 34 Global Attack Surface Management (ASM) Market Outlook, By Exposure Assessment (2023-2034) (\$MN)

Table 35 Global Attack Surface Management (ASM) Market Outlook, By Threat Intelligence Integration (2023-2034) (\$MN)

Table 36 Global Attack Surface Management (ASM) Market Outlook, By Compliance & Governance (2023-2034) (\$MN)

Table 37 Global Attack Surface Management (ASM) Market Outlook, By Incident Response Support (2023-2034) (\$MN)

Table 38 Global Attack Surface Management (ASM) Market Outlook, By End User (2023-2034) (\$MN)

Table 39 Global Attack Surface Management (ASM) Market Outlook, By BFSI (2023-2034) (\$MN)

Table 40 Global Attack Surface Management (ASM) Market Outlook, By Government & Defense (2023-2034) (\$MN)

Table 41 Global Attack Surface Management (ASM) Market Outlook, By Healthcare & Life Sciences (2023-2034) (\$MN)

Table 42 Global Attack Surface Management (ASM) Market Outlook, By IT & Telecommunications (2023-2034) (\$MN)

Table 43 Global Attack Surface Management (ASM) Market Outlook, By Manufacturing (2023-2034) (\$MN)

Table 44 Global Attack Surface Management (ASM) Market Outlook, By Retail & E-commerce (2023-2034) (\$MN)

Table 45 Global Attack Surface Management (ASM) Market Outlook, By Energy & Utilities (2023-2034) (\$MN)

Table 46 Global Attack Surface Management (ASM) Market Outlook, By Media & Entertainment (2023-2034) (\$MN)

Table 47 Global Attack Surface Management (ASM) Market Outlook, By Education (2023-2034) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) are also represented in the same manner as above.

I would like to order

Product name: Attack Surface Management (ASM) Market Forecasts to 2034 – Global Analysis By Offering (Software/Platform and Services), Deployment Mode, Asset Type, Attack Surface Type, Application, End User and By Geography

Product link: <https://marketpublishers.com/r/AF82B40D1103EN.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/AF82B40D1103EN.html>