

## **Adaptive Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)**

Market Report | 2025-06-01 | 119 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:**

Adaptive Security Market Analysis

The adaptive security market is valued at USD 14.38 billion in 2025 and is forecast to reach USD 32.27 billion by 2030, advancing at a robust 17.54% CAGR. This expansion mirrors the rapid shift from perimeter-centric defenses to self-learning architectures that analyze user behavior, asset context, and threat intelligence in real time. Government zero-trust mandates, sharper regulatory penalties, and an unprecedented rise in AI-driven attack traffic are forcing enterprises to retire static controls and adopt continuously tuned safeguards. Vendors are embedding large-language-model reasoning, automated policy orchestration, and behavior analytics into unified platforms, reducing mean time to detect and respond while lowering administrative overhead. Organic demand is amplified by mounting board-level concern over brand damage and ransomware payouts that routinely exceed the cost of proactive controls.

Global Adaptive Security Market Trends and Insights

AI-Generated Attack Traffic Outpacing Rule-Based Defenses

AI-enabled adversaries now automate phishing, vulnerability discovery, and lateral movement, generating traffic patterns that evade signature-based tools. CrowdStrike launched agentic AI modules in 2025 that autonomously hunt and contain never-seen malware across endpoints and cloud workloads. Darktrace's autonomous response engine already blocks suspicious sessions mid-stream, such as its 2025 mitigation of ClickFix phishing waves. These proof points illustrate how real-time behavior models

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scott-international.com](mailto:support@scott-international.com)

[www.scott-international.com](http://www.scott-international.com)

supersede static rule sets, cementing demand for adaptive security market solutions that refine policies without human tuning.

### Regulatory Mandates Driving Compliance-Driven Security Investments

The EU NIS2 and DORA regulations that took effect in 2025 impose fines up to EUR 10 million or 2% of global turnover for inadequate cyber controls, forcing banks, utilities, and digital service providers to implement continuous monitoring and least-privilege access. U.S. federal agencies face identical pressure under Executive Order 14028, with CISA's Zero-Trust Maturity Model detailing phased milestones through fiscal 2027. The U.S. Department of Defense complements this with a mandatory zero-trust framework for all networks by 2027. Together, these mandates create a multiplier effect that boosts the adaptive security market as firms seek unified platforms capable of mapping a single control to multiple regulations.

### Shortage of Skilled Cybersecurity Talent

There are nearly 600,000 unfilled U.S. cybersecurity roles, and experienced practitioners enjoy zero percent unemployment, according to Varonis' 2025 labor snapshot. Small firms and Asian SMEs struggle most, with Japan's 2024 SME survey showing staff shortages as the top cyber-readiness barrier. This gap encourages managed detection and response services and fuels the 17.8% CAGR forecast for the Services segment within the adaptive security market. Fortinet answered the skills crunch by embedding GenAI playbooks into FortiAnalyzer 2025, enabling lean teams to triage alerts that formerly required senior analysts.

Other drivers and restraints analyzed in the detailed report include:

Enterprise Cloud and SaaS Sprawl Necessitating Zero-Trust Controls / Surge in Machine-to-Machine Identities Requiring Continuous Risk Scoring / High TCO and Integration Complexity for Brownfield IT Estates /

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

### Segment Analysis

Adaptive security market size for Application Security stood at USD 5.23 billion in 2024 and preserved a 36.4% slice of revenue owing to heightened API exploitation. Akamai's 2025 Apps and API report revealed that APIs account for 57% of all observed traffic and are increasingly weaponized. Enterprises therefore deploy runtime inspection, schema validation, and behavior baselining to block injection attacks that bypass perimeter gateways. Cloud Security, meanwhile, advances at an 18.1% CAGR as zero-trust policy engines embed directly into container orchestrators and serverless runtimes, giving DevOps teams native safeguards. Vendors such as Syncloop layer unsupervised anomaly detection over Kubernetes clusters, reducing false positives and easing SOC fatigue. Network and endpoint controls remain essential but converge into platform bundles so buyers can streamline telemetry pipelines and automate kill-chain disruption.

Despite Solutions retaining 62.6% of 2024 sales, the adaptive security market size for Services will grow faster as boards outsource detection, response, and compliance reporting to experts. Skills shortages and 24/7 coverage needs push even Fortune 500 firms toward managed orchestration. Ciena's case study on optical network customers shows service providers packaging AI-driven threat analytics into connectivity deals, offloading capex and skill burdens for industrial clients. Service providers leverage multitenant SIEMs and AIOps to reduce per-customer cost and expand gross margin, reinforcing a cycle where technology buyers prefer outcomes over tool ownership.

Adaptive Security Market is Segmented by Application (Application Security, Network Security, and More), Offering (Solutions and Services), Deployment Model (On-Premises and Cloud-Based), End User (BFSI, Government and Defense, and More), and by Geography. The Market Forecasts are Provided in Terms of Value (USD).

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

## Geography Analysis

North America's 32.8% share stems from early zero-trust pilots, venture funding depth, and federal spending. Executive Order 14028 and CISA guidance obligate federal agencies to deploy continuous authentication, spurring private-sector imitation in supply chains. Microsoft provides prescriptive blueprints for agencies migrating to Security Copilot, accelerating best-practice diffusion across the region. Local talent pools and a well-developed cyber-insurance market also sustain premium pricing for high-assurance products.

Asia-Pacific is set for the fastest climb at a 19.3% CAGR through 2030. Japan's Cybersecurity Strategy Council earmarked JPY 1.2 trillion for public-private R&D programs, fostering domestic vendors that integrate post-quantum cryptography and threat-intel sharing. Singapore's Smart Nation blueprint injects funding for AI SOC automation, while multinational manufacturers relocate facilities to Southeast Asia and demand adaptive safeguards for smart factories. China's dominance in AI security patents, accounting for 70% of 2023 global filings, puts pressure on neighbors to accelerate local innovation and cross-border threat-sharing pacts.

Europe records solid growth on the back of regulatory heft. NIS2 forces energy, water, and transport operators to verify supply-chain hardening, while DORA extends similar rules to financial entities. ENISA's 2025 survey showed 86% policy adoption but only 47% budget allocation, implying pent-up demand for turnkey managed services. The upcoming Cyber Resilience Act broadens coverage to all digital products, fueling fresh procurements among consumer-electronics manufacturers.

### List of Companies Covered in this Report:

Cisco Systems / IBM Corp. / Fortinet / Palo Alto Networks / Trend Micro / Rapid7 / Check Point Software / Juniper Networks / Trellix / CrowdStrike / Zscaler / Illumio / Lumen Technologies / Aruba (HPE) / Microsoft Security / Okta / Netskope / Darktrace / Akamai / Guardicore / WatchGuard (Panda) /

### Additional Benefits:

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

### Table of Contents:

- 1 INTRODUCTION
  - 1.1 Study Assumptions and Market Definition
  - 1.2 Scope of the Study
- 2 RESEARCH METHODOLOGY
- 3 EXECUTIVE SUMMARY
- 4 MARKET LANDSCAPE
  - 4.1 Market Overview
  - 4.2 Market Drivers
    - 4.2.1 Escalating volume and sophistication of cyber-attacks
    - 4.2.2 Regulatory mandates (GDPR, CCPA, DORA, NIS2, etc.)
    - 4.2.3 Enterprise cloud and SaaS sprawl needing zero-trust controls

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

- 4.2.4 AI-generated attack traffic outpacing rule-based defenses
- 4.2.5 Surge in machine-to-machine identities requiring continuous risk scoring
- 4.2.6 5G network-slicing driving micro-segmentation adoption
- 4.3 Market Restraints
  - 4.3.1 Shortage of skilled cyber-security talent
  - 4.3.2 High TCO and integration complexity for brown-field IT estates
  - 4.3.3 Legacy OT/ICS environments with proprietary protocols
  - 4.3.4 Data-sovereignty conflicts in multi-cloud deployments
- 4.4 Supply-Chain Analysis
- 4.5 Regulatory Landscape
- 4.6 Technological Outlook (AI, UEBA, SSE, micro-segmentation, PQC)
- 4.7 Porter's Five Force Analysis
  - 4.7.1 Bargaining Power of Suppliers
  - 4.7.2 Bargaining Power of Buyers
  - 4.7.3 Threat of New Entrants
  - 4.7.4 Threat of Substitutes
  - 4.7.5 Competitive Rivalry
- 4.8 Assessment of Macroeconomic Trends on the Market

## 5 MARKET SIZE AND GROWTH FORECASTS (VALUE)

- 5.1 By Application
  - 5.1.1 Application Security
  - 5.1.2 Network Security
  - 5.1.3 Endpoint Security
  - 5.1.4 Cloud Security
  - 5.1.5 Others
- 5.2 By Offering
  - 5.2.1 Solutions
  - 5.2.2 Services
- 5.3 By Deployment Model
  - 5.3.1 On-premise
  - 5.3.2 Cloud-based
- 5.4 By End User
  - 5.4.1 BFSI
  - 5.4.2 Government and Defense
  - 5.4.3 Manufacturing (Industry 4.0)
  - 5.4.4 Healthcare and Life Sciences
  - 5.4.5 Energy and Utilities
  - 5.4.6 Others
- 5.5 By Geography
  - 5.5.1 North America
    - 5.5.1.1 United States
    - 5.5.1.2 Canada
    - 5.5.1.3 Mexico
  - 5.5.2 South America
    - 5.5.2.1 Brazil
    - 5.5.2.2 Argentina

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

- 5.5.2.3 Rest of South America
- 5.5.3 Europe
  - 5.5.3.1 United Kingdom
  - 5.5.3.2 Germany
  - 5.5.3.3 France
  - 5.5.3.4 Sweden
  - 5.5.3.5 Rest of Europe
- 5.5.4 Asia-Pacific
  - 5.5.4.1 China
  - 5.5.4.2 Japan
  - 5.5.4.3 India
  - 5.5.4.4 Australia
  - 5.5.4.5 South Korea
  - 5.5.4.6 Rest of Asia-Pacific
- 5.5.5 Middle East and Africa
  - 5.5.5.1 Saudi Arabia
  - 5.5.5.2 United Arab Emirates
  - 5.5.5.3 Turkey
  - 5.5.5.4 South Africa
  - 5.5.5.5 Rest of Middle East and Africa

## 6 COMPETITIVE LANDSCAPE

- 6.1 Market Concentration
- 6.2 Strategic Moves (MandA, funding, product launches)
- 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, Products and Services, Recent Developments)
  - 6.4.1 Cisco Systems
  - 6.4.2 IBM Corp.
  - 6.4.3 Fortinet
  - 6.4.4 Palo Alto Networks
  - 6.4.5 Trend Micro
  - 6.4.6 Rapid7
  - 6.4.7 Check Point Software
  - 6.4.8 Juniper Networks
  - 6.4.9 Trellix
  - 6.4.10 CrowdStrike
  - 6.4.11 Zscaler
  - 6.4.12 Illumio
  - 6.4.13 Lumen Technologies
  - 6.4.14 Aruba (HPE)
  - 6.4.15 Microsoft Security
  - 6.4.16 Okta
  - 6.4.17 Netskope
  - 6.4.18 Darktrace
  - 6.4.19 Akamai / Guardicore
  - 6.4.20 WatchGuard (Panda)

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

## 7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK

### 7.1 White-space and Unmet-need Assessment

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

**Adaptive Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)**

Market Report | 2025-06-01 | 119 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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-02-26"/>
		Signature	

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

