Cybersecurity Software - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-02-09 | 100 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:

Cybersecurity Software Market Analysis

The cybersecurity software market size in 2026 is estimated at USD 159.99 billion, growing from 2025 value of USD 141.13 billion with 2031 projections showing USD 299.42 billion, growing at 13.36% CAGR over 2026-2031. Cloud-first mandates, rising adoption of zero-trust frameworks, and the growing volume of AI-enabled attacks are reinforcing demand for unified security platforms. Cloud deployment models already command two-thirds of total spending, while platform consolidation continues as enterprises reduce tool sprawl and seek measurable risk reduction. Escalating regulatory fines and incident-disclosure rules are accelerating procurement decisions, and proactive investment is spreading from large enterprises to small and medium businesses. Vendors that integrate identity, cloud, and analytics functions into a single architecture are capturing outsized opportunity within the cybersecurity software market.

Global Cybersecurity Software Market Trends and Insights

Cloud-first Adoption and Zero-trust Mandates

Zero-trust frameworks are moving from strategic vision to operational reality, with 81% of organizations planning deployments by 2026. Major providers now embed security-by-design into cloud services, and Microsoft's cybersecurity revenue surpassed USD 20 billion in 2024, underscoring vendor momentum. Analysts confirm that 68% of recent industrial incidents started with IT system compromise, tightening the link between zero-trust projects and operational resilience. Multicloud complexity is prompting

enterprises to favor unified policy enforcement across environments, which is driving up demand for integrated platforms. Providers that combine identity, access, and network segmentation within a single stack are gaining procurement preference. The result is a steady uptick in long-term contracts that lock in platform subscriptions.

Surge in AI-driven, Multi-vector Cyber-attacks

Information-stealing malware cases spiked 500% in 2024, while ransomware-as-a-service shops lowered entry barriers for attackers. API vulnerabilities rose 1,205% as adversaries automated reconnaissance and exploitation, overwhelming traditional defenses. The high-profile Change Healthcare breach affected 100 million people and involved a USD 22 million ransom payment, demonstrating the business impact of AI-enabled campaigns. CrowdStrike now processes 84 trillion daily threat signals to sharpen predictive analytics, reflecting escalating arms-race dynamics. Boards increasingly treat AI-driven risk as a strategic threat, translating into budget protection even amid broader IT spending reviews.

Persistent Talent Deficit and Wage Inflation

Japan alone needs over 200,000 additional cybersecurity professionals, and specialists there earn about USD 135.50 per hour, up from prior levels. Operational-technology security skills are scarcer still, even as OT attacks rose 73% in 2024. Companies are shifting to managed security services and to AI-based automation to fill gaps, but both require cultural change and onboarding investments. The shortfall increases the total cost of ownership for advanced security programs and slows large-scale rollouts. Over time, persistent wage pressure will influence vendor pricing models and could moderate the cybersecurity software market growth rate.

Other drivers and restraints analyzed in the detailed report include:

Expanding Regulatory Fines and SEC Incident-disclosureTool Sprawl Causing ROI Fatigue in C-suites

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

Segment Analysis

Identity and Access Management commanded 25.10% of the cybersecurity software market share in 2025, illustrating that identity is now the primary control plane for enterprise defense. Cloud security solutions are forecast to register a 14.60% CAGR through 2031, the fastest of all offerings, as businesses secure multicloud and hybrid workloads. CyberArk's USD 1.54 billion acquisition of Venafi spotlights the growing importance of machine-identity governance. The cybersecurity software market size tied to application and data security is also rising as DevSecOps gains ground and privacy regulations tighten.

Demand is coalescing around integrated platforms that span identity, cloud, data, and infrastructure layers. Infrastructure and network protection remains core for hybrid environments, while emerging post-quantum cryptography solutions move from labs to pilots after NIST finalized three quantum-resistant algorithms in 2024. Customers increasingly prefer vendors that can knit multiple functions into a single control fabric to lower operational overhead.

Cloud deployments captured 66.85% share in 2025 and are expected to grow at 13.62% CAGR through 2031, cementing irreversible migration trends in the cybersecurity software market. Microsoft enhanced Azure with AI threat analytics and post-quantum encryption, showing how hyperscalers embed advanced capabilities directly into their stacks. On-premises implementations decline steadily yet persist where regulatory data-residency rules apply.

Hybrid strategies combine cloud agility with on-site controls for sensitive workloads such as patient data. Healthcare organizations

moved decisively to cloud security after seeing a 300% jump in attacks since 2015. Edge computing is emerging as a third pillar requiring location-aware policy enforcement. Vendors able to protect workloads consistently across cloud, on-premises, and edge win favor in procurement cycles.

Cybersecurity Software Market is Segmented by Offering (Application Security, Cloud Security, Data Security and More), Deployment Model (On-Premises, Cloud), End-User Vertical (BFSI, Healthcare, Manufacturing and More), Organization Size (Large Enterprises, Small and Medium Enterprises (SMEs)), and by Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America accounts of 24.35% the largest regional share through a mature vendor ecosystem, strong venture funding, and regulatory mandates such as SEC incident-disclosure rules. Microsoft's security revenue surpassed USD 20 billion, and CrowdStrike reported USD 4.6 billion annual recurring revenue in 2025, showcasing regional scale. Cross-border supply-chain requirements are boosting adoption in Canada and Mexico. Cyber-insurance premiums have stabilized, suggesting improving baseline defenses across enterprises.

Asia-Pacific is the fastest-growing region with a 13.42% CAGR through 2031, driven by rapid digitization and elevated threat volume that accounts for 31% of global incidents. China's cybersecurity outlays are projected to top USD 38.6 billion by 2023, propelled by government directives. Japan expects a USD 13.25 billion market by 2029 but faces significant talent shortages. South Korea nurtures innovative startups like AI SPERA, which raised USD 8.5 million to scale its Criminal IP platform. The region's cyber-insurance premiums are growing near 50% annually, signaling maturation of risk-transfer mechanism.

Europe shows steady expansion under GDPR, NIS2, and emerging AI regulations requiring demonstrable controls. Germany, the United Kingdom, and France lead spending, while Eastern European states accelerate adoption amid EU integration. The Middle East and Africa exhibit high-growth pockets, led by Gulf Cooperation Council smart-city projects and national cyber strategies in the UAE and Saudi Arabia. South Africa, Nigeria, and Egypt are early continental leaders, though workforce development remains a constraint. Vendors that localize offerings to data-sovereignty rules and language preferences stand to gain within these emerging sub-regions.

List of Companies Covered in this Report:

IBM Microsoft Cisco Check Point Broadcom (Symantec) Fortinet F5 Palo Alto Networks Proofpoint CyberArk Zscaler Mandiant (Google) Sophos CrowdStrike Okta Cloudflare Trend Micro Rapid7 SentinelOne Qualys

Additional Benefits:

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

Table of Contents:

5.4.2 Small and Medium Enterprises (SMEs)
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
5.5.2.3 Rest of South America
5.5.3 Europe
5.5.3.1 Germany
5.5.3.2 United Kingdom
5.5.3.3 France
5.5.3.4 Italy
5.5.3.5 Spain
5.5.3.6 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 South Korea
5.5.4.5 Australia
5.5.4.6 Southeast Asia
5.5.4.7 Rest of Asia-Pacific
5.5.5 Middle East and Africa
5.5.5.1 Middle East
5.5.5.1.1 Saudi Arabia
5.5.5.1.2 United Arab Emirates
5.5.5.1.3 Turkey
5.5.5.1.4 Rest of Middle East
5.5.5.2 Africa
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 IBM
6.4.2 Microsoft
6.4.3 Cisco
6.4.4 Check Point

Cybersecurity Software - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-02-09 | 100 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	2026-02-27
		Signature