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

Market Report | 2025-07-01 | 120 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:

Application Security Market Analysis

The application security market was valued at USD 13.64 billion in 2025 and is expected to reach USD 30.41 billion by 2030, advancing at a 17.39% CAGR. Cloud migration, API-centric software design and expanding regulatory mandates are accelerating adoption across every major industry vertical. Growth is reinforced by a sharp increase in API traffic, the widespread use of AI-generated code and heightened incident disclosure rules that force organizations to strengthen testing earlier in the development life cycle. Large enterprises continue to anchor overall spending, yet managed platforms aimed at small and medium enterprises (SMEs) are opening a sizeable new addressable base for vendors. Technology convergence is reshaping competitive dynamics, with platform providers integrating static, dynamic and runtime protection to curb tool sprawl and improve developer productivity.

Global Application Security Market Trends and Insights

Rising Volume and Sophistication of Web, Mobile and API-Based Attacks

Web application attacks in the Asia-Pacific region surged 73% to 51 billion events in 2024, underscoring how attackers now exploit APIs at scale. Retailers developing more than 1,000 APIs yearly confront an enlarged attack surface that bypasses perimeter controls. Supply-chain breaches climbed 431% between 2021 and 2023, demonstrating a pivot toward dependency exploitation rather than direct code injection. Enterprises are integrating runtime application self-protection with behavioral analytics to act on anomalous traffic patterns rather than static signatures. Manufacturing recorded a 79% API incident rate, confirming that adversaries move faster than most operational technology security programs.

Rapid Adoption of DevSecOps Toolchains

DevSecOps penetration rose from 27% in 2020 to 36% in 2024 as teams embed testing earlier in continuous integration pipelines. Platforms processing billions of findings, such as ArmorCode, apply machine learning to correlate vulnerabilities and prioritize remediation at scale. Despite progress, 78% of enterprises report "shift-left fatigue," aggravated by redundant tools that overwhelm developers with alerts. The most effective programs streamline security tasks inside integrated development environments, treating policies as version-controlled artifacts automatically enforced at commit. This model is extending through AI assistants that suggest fixes inside code editors, thereby reducing context-switch time between development and security portals.

High Total Cost of Ownership and Tool Complexity

Software-as-a-service inflation reached 11.3% in 2024, with some vendors lifting prices by 25%.Forty-two percent of SMEs still lack a structured incident response plan, revealing budget constraints that limit enterprise-grade controls. Organizations deploy overlapping scanners, agents and policy engines that demand scarce integration skills, leading 89% of firms to foresee additional staffing needs despite flat headcounts. Managed platforms such as Contrast One now bundle expert services with tooling to cut administrative overhead. Consumption-based pricing models are also emerging, enabling smaller businesses to align spending with actual test frequency.

Other drivers and restraints analyzed in the detailed report include:

Expanding Regulatory Mandates / Growth in Third-Party SaaS Integrations / Global Shortage of Secure-Coding Talent /

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

Segment Analysis

Solutions retained a 78.5% share in 2024, reflecting enterprise preference for integrated suites. Market leaders combine SAST, DAST, IAST and RASP under one license to limit tool sprawl. Consolidated dashboards reduce context switching and speed decision-making, fixing a common pain point cited by development teams. The service segment, though smaller, outran the broader application security market with a 17.9% CAGR and will continue to benefit from skills gaps.

Demand for managed security accelerates within SMEs that cannot afford full-time specialists. Providers use predictable subscription pricing and outcome-based service-level agreements to attract cost-conscious buyers. For large enterprises, professional services focus on policy mapping, pipeline integration and red-team simulations that validate runtime defenses. Vendors also introduce consumption-tiered offerings, letting customers buy scanning credits rather than perpetual seats, bringing transparency to budgeting for vulnerability management.

Cloud deployment controlled 65.9% of the application security market in 2024 and is forecast to advance at a 19.3% CAGR. DORA and related regulations specify four-hour incident reporting, a timeline difficult to meet without centralized logging and scalable analytics. Cloud-native solutions enable rapid rollout of policy updates and integrate easily with container orchestration systems.

On-premises solutions remain prevalent in defense and public-sector workloads that require data residency. Hybrid patterns are growing as financial firms keep sensitive workloads on private infrastructure while using cloud scanners during development.

Cloud vendors invest in hardware-backed attestation and confidential computing to address lingering sovereignty concerns. Competition now centers on alignment with cloud security posture management functions that map misconfigurations across both infrastructure and application layers.

Application Security Market is Segmented by Application Type (Web Application Security, and More), Component (Solutions, Services), Deployment Mode (Cloud, On-Premises), Organization Size (SMEs, Large Enterprises), Security Testing Type (SAST, DAST, and More), End-User Industry (BFSI, Healthcare, Retail and E-Commerce, and More), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America led the application security market with a 28.9% revenue share in 2024, underpinned by strong regulatory pressure and average Fortune 500 security budgets exceeding USD 20 million annually. Enterprises integrate zero-trust architectures that merge identity, network and application controls to support remote and hybrid work. Advancements originate in technology hubs where vendors pilot AI-driven vulnerability correlation workloads, delivering faster mean time to remediation.

Asia-Pacific records the fastest projected 17.5% CAGR through 2030, fueled by digital government programs, rising fintech adoption and a 73% spike in web application attacks that hit 51 billion events in 2024. Governments in Singapore and India release refreshed cyber strategies that map minimum control baselines for critical infrastructure. The region's manufacturing sector, despite lower digital maturity, faces the highest share of API incidents, pushing vendors to localize threat intelligence and language-specific remediation resources.

Europe's momentum hinges on comprehensive statutes such as DORA, the Cyber Resilience Act and GDPR. Financial entities must implement ICT risk management frameworks and deliver four-hour breach notifications from January 2025. Organizations allocate around 9% of IT budgets to information security, yet 89% still anticipate hiring increases to meet these mandates. Hybrid deployment preferences persist because data-sovereignty clauses encourage on-premise processing of sensitive workloads while permitting cloud-based analytics for less critical data.

List of Companies Covered in this Report:

IBM / Synopsys Inc. / Checkmarx / Veracode (Thoma Bravo) / Micro Focus / Oracle Corporation / Rapid7 / Qualys / Palo Alto Networks / Fortinet / Trend Micro / GitLab / GitHub / Snyk / CrowdStrike / Contrast Security / WhiteHat Security (NTT) / Positive Technologies / SiteLock / Mend (WhiteSource) / ArmorCode / Fasoo / HCL Software (AppScan) /

Additional Benefits:

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

Table of Contents:

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

Market Report | 2025-07-01 | 120 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	