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

Market Report | 2025-06-01 | 124 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:

Software Defined Security Market Analysis

The software-defined security market size is estimated at USD 12.9 billion in 2025 and is forecast to more than double to USD 26.91 billion by 2030, advancing at a 15.84% CAGR. Most enterprises are moving away from perimeter-centric controls toward programmable architectures that follow workloads as they shift across data centers, multiple public clouds, and edge locations. Automated policy enforcement shortens incident-response cycles, while zero-trust principles embed continuous verification into everyday network operations. Regulatory deadlines such as the EU Cyber Resilience Act and the NIS2 Directive are converting discretionary spending into mandatory investments. At the same time, the rapid growth of containerized applications forces security teams to embrace granular micro-segmentation and runtime protection that only software-defined approaches can deliver. Together, these forces give the software-defined security market durable, double-digit momentum through the end of the decade.

Global Software Defined Security Market Trends and Insights

Requirement for quicker incident response and policy automation

Mean time to detection must now be measured in minutes, not days. Coalition's 2025 Cyber Threat Index found that 58% of ransomware intrusions began with compromised VPN devices, exposing the limits of manual responses. Enterprises therefore employ programmable security controls that auto-isolate endpoints once threat intelligence crosses defined risk thresholds. The

financial stakes remain high: average breach costs in Canada reached USD 4.66 million and churn rates climbed to 38% among affected customers in 2025. Automated, software-defined playbooks let security teams scale without proportional head-count increases, aligning protection speed with adversary tempo.

Rising adoption of multi-cloud and hybrid cloud architectures

Nutanix reports that 90% of global organizations now run a "cloud-smart" mix of private and multiple public clouds [nutanix.com]. Such diversity fragments visibility; 71% of teams acknowledge policy blind spots in at least one environment. Software-defined security platforms resolve that fragmentation by abstracting policy from the underlying infrastructure. Unified dashboards apply identical controls regardless of whether workloads run on-premises, AWS, Azure, or OCI, ensuring continuous compliance while giving developers freedom to place applications where they perform best.

Shortage of DevSecOps talent

O'Reilly's 2024 survey shows 38.9% of organizations citing cloud security skills as their biggest gap. DevSecOps engineer salaries in the United States already average USD 140,000, pressuring budgets and project timelines. Many firms backfill the gap with managed service providers, which boosts the services segment but slows in-house adoption of advanced features.

Other drivers and restraints analyzed in the detailed report include:

Surge in container/Kubernetes security spend / National cyber-resilience mandates after critical-infrastructure attacks / Legacy-system interoperability issues /

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

Segment Analysis

Public cloud continues to lead overall penetration, delivering 39% of 2024 revenue. Within that category, the SaaS-only slice is climbing fastest at an 18.20% CAGR. Smaller IT teams in particular prize the instant scaling and rolling updates that cloud-native vendors provide, since no on-premises appliances require patching. Larger enterprises also shift workloads into SaaS nodes to reduce capex and accelerate feature adoption as zero-trust frameworks mature.

On-premises deployments remain indispensable where sovereignty or latency mandates apply; however, hybrid designs increasingly route outbound traffic through SaaS secure web gateways. Combined, these trends move policy control toward the network edge and favour vendors that architect multi-tenant, elastic backplanes. The transition underscores the broader repositioning of the software defined security market from appliance sales to subscription revenue.

Network security still represents 40% of 2024 revenue, reflecting legacy firewall refresh cycles and software-defined wide-area network rollouts. The higher-growth story lies in cloud/container security, which will expand at a 24% CAGR through 2030. Development teams containerize monoliths into hundreds of microservices, so runtime controls must adapt in seconds as pods respawn. Continuous image scanning, admission-control hooks, and service-mesh encryption therefore top procurement lists.

Early adopters increasingly bundle container security with posture-management modules that inventory misconfigurations across AWS, Azure, and Google Cloud. This convergence further blurs lines between workload and configuration security, pushing vendors to integrate cloud-native application protection platforms directly into their broader software defined security market suites.

Software Defined Security Market Report is Segmented by Component (Software, Services), Deployment Model (On-Premises, Public Cloud and More), Security Type (Network Security, Endpoint Security and More), Organization Size (Small & Medium Enterprises and Large Enterprises), End User (BFSI, Telecommunications & IT and More) and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America captured 38% of 2024 revenue, underpinned by decisive federal action. The U.S. Department of Defense allocated USD 504.9 million to DISA cyber operations for fiscal 2025, with a mandate to build zero-trust reference architectures that ripple into contractor ecosystems. Corporate boards mirror that urgency: overall cybersecurity spending in the region grew 15% year over year, buoyed by the White House's executive orders that require software bills of materials and continuous monitoring across the federal supply chain.

Europe sits in second place but posts healthy acceleration as the software defined security market aligns with sweeping legislation. The Cyber Resilience Act coming into force in December 2027 obliges manufacturers to design products with security baked in from day one. Complementary measures such as the Digital Operational Resilience Act (for finance) and NIS2 (for essential services) extend similar obligations across the economy. Enterprises are therefore converging on programmable policy engines capable of proving compliance in real time to multiple supervisory bodies.

Asia-Pacific is the growth frontrunner, set to log a 14.90% CAGR through 2030. Manufacturing heavyweights in China, Japan, and South Korea pursue Industry 4.0 programs that expose operational-technology networks to internet threats. Governments respond with sector-specific frameworks that recommend micro-segmentation and zero-trust, propelling new projects. India's Digital Personal Data Protection Act similarly raises bars for healthcare and e-commerce operators. Collectively, these moves expand the regional share of the global software defined security market.

The Middle East, Africa, and South America are emerging adopters. Energy exporters commission secure-by-design refinery control systems, while Brazilian financial regulators publish stringent open-banking security guidelines. Although absolute spend remains lower, high growth rates make these geographies attractive for cloud-native vendors seeking greenfield opportunities.

List of Companies Covered in this Report:

Palo Alto Networks / Cisco Systems / Fortinet / Juniper Networks / VMware (Broadcom) / Check Point Software / IBM / Oracle / Microsoft / Trend Micro / Huawei / Sophos / McAfee / Splunk / Illumio / Akamai Technologies / Netskope / Zscaler / Forcepoint / Darktrace / Proofpoint /

Additional Benefits:

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

Table of Contents:

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

Market Report | 2025-06-01 | 124 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	2026-02-26
		Signature