Network Security Market By Solution (Firewall/Next Generation Firewall, Secure Web Gateways, Unified Threat Management, Network Detection & Response, Network Access Control), Network Environment (Branch, Campus, Data Center)- Global Forecast to 2030

Market Report | 2025-12-05 | 465 pages | MarketsandMarkets

AVAILABLE LICENSES:

- Single User $4950.00
- Multi User $6650.00
- Corporate License $8150.00
- Enterprise Site License $10000.00

Report description:

The network security market is projected to grow from USD 84.50 billion in 2025 to USD 119.70 billion by 2030 at a Compound Annual Growth Rate (CAGR) of 7.2% during the forecast period. The market is driven by the increasing frequency and sophistication of cyberattacks targeting hybrid networks, cloud workloads, and encrypted traffic, prompting organizations to strengthen both perimeter and internal defenses. At the same time, the growing BYOD trend is expanding enterprise attack surfaces as personal devices connect to corporate environments, necessitating the implementation of strict access controls, continuous monitoring, and advanced threat prevention. Together, these factors accelerate the adoption of next-generation network security solutions across industries.

https://mnmimg.marketsandmarkets.com/Images/network-security-market-img-overview.webp

"By network environment, the data center network security segment is expected to hold the largest market size during the forecast period."
Data center network security is expected to be the largest segment in the network environment because data centers house the bulk of sensitive workloads, large volumes of structured/unstructured data, virtualized environments, and mission-critical applications. As enterprises consolidate operations, virtualize servers, and adopt hybrid cloud strategies, data centers become high-value targets for attackers, including advanced persistent threats, insider threats, and lateral movement attacks, as well as data exfiltration, DDoS, and application-layer breaches. To safeguard these assets, organizations deploy robust security

measures, including segmentation, micro-segmentation, intrusion detection/prevention, next-generation firewalls, secure access controls, and continuous monitoring. The importance of uptime, regulatory compliance, data confidentiality, and performance optimization ensures that data-center security remains central. Given the concentration of risk and value, data center network security continues to command the largest share of network security investments.

"By vertical, the cloud segment is projected to register the highest CAGR during the forecast period."

The healthcare and life sciences vertical is the fastest-growing sector due to rising digitization, regulatory pressure such as data privacy laws, the adoption of telemedicine, cloud-based patient data management, and the increasing interconnectedness of medical devices (IoMT - Internet of Medical Things). Hospitals, laboratories, and research institutions handle sensitive patient data, intellectual property, and mission-critical systems. The growing frequency of ransomware attacks, data breaches, and disruption risks necessitates the implementation of advanced security measures, including encryption, zero-trust access, secure network segmentation, cloud security, and continuous monitoring. As healthcare organizations modernize, move to cloud-based record systems, and collaborate globally, they require scalable, reliable, and compliant network security, prompting a surging demand and positioning the healthcare & life sciences sector as the fastest-growing vertical in the network security market.

By deployment mode, the on-premises segment is expected to lead in terms of market share during the forecast period.

On-premises deployment remains the dominant deployment mode in network security because many organizations, especially large enterprises, government institutions, and regulated industries, prefer full control over their security infrastructure, data residency, performance, and latency. On-premises setups allow organizations to integrate security tools tightly with legacy systems, internal networks, and existing infrastructure. They can customize configurations, enforce strict access policies, and apply segmentation in ways that suit internal governance rules. For compliance-driven sectors such as banking, finance, and government, data sovereignty and regulatory mandates often require sensitive data to remain on-site. Additionally, on-premises deployments eliminate potential cloud-related latency, visibility, or vendor dependency issues. Because of these factors, many enterprises continue to rely on on-premises security infrastructure, sustaining its position as the largest deployment mode segment.

Breakdown of Primaries

The study draws insights from a range of industry experts, including component suppliers, Tier 1 companies, and OEMs. The break-up of the primaries is as follows:

- By Company Type: Tier 1 - 40%, Tier 2 - 35%, and Tier 3 - 25%
- By Designation: Directors - 45%, Managers - 35%, Others - 20%
- By Region: North America - 35%, Europe - 30%, Asia Pacific - 25%, Middle East & Africa - 5%, Latin America - 5%

Major vendors in the network security market include Cisco (US), Palo Alto Networks (US), Fortinet (US), Check Point (US), Trend Micro (Japan), Verizon (US), IBM (US), Broadcom (US), Juniper Networks (US), Akamai (US), Netskope (US), Microsoft (US), CrowdStrike (US), Zscaler (US), Cloudflare (US), AWS (US), OpenText (Canada), Hillstone Networks (US), Barracuda Networks (US), Huawei (China), Trellix (US), SonicWall (US), Forcepoint (US), Sophos (UK), Ivanti (US), Extreme Networks (US), Zyxel Networks (Taiwan), Cato Networks (Israel), NordLaver (US), Versa Networks (US), WiJungle (India), Cynet (US), SECNAP Network Security (US), Nomios (Netherlands), easi (Belgium), GajShield (India), Stellar Cyber (US), NETSCOUT (US), and Fidelis Security (US).

The study includes an in-depth competitive analysis of the key players in the network security market, their company profiles, recent developments, and key market strategies.

Research Coverage

The report segments the network security market and forecasts its size based on solution (firewall/next-generation firewall, virtual private network, network access control, data loss prevention, intrusion detection/intrusion prevention systems, secure web gateways, distributed denial-of-service mitigation, unified threat management, network detection & response, and other solutions such as URL/content filtering, web/DNS filtering, and vulnerability scanning), service (professional services-including design, consulting & implementation, risk & threat assessment, training & education, support & maintenance-and managed services), network environment (branch, campus, and data center network security), deployment mode (cloud, on-premises, and hybrid), organization size (large enterprises and small & medium-sized enterprises), and vertical (BFSI, government, healthcare & life sciences, manufacturing, IT & ITeS, retail & e-commerce, energy & utilities, telecommunications, transportation & logistics, media & entertainment, aerospace & defense, and other verticals such as education, construction, real estate, and travel & hospitality).

The study also includes an in-depth competitive analysis of the market's key players, their company profiles, key observations related to product and business offerings, recent developments, and key market strategies.

Key Benefits of Buying the Report

The report will help market leaders/new entrants with information on the closest approximations of revenue numbers for the overall network security market and its subsegments. This report will help stakeholders understand the competitive landscape and gain valuable insights to better position their businesses and plan suitable go-to-market strategies. The report also helps stakeholders understand the market pulse and provides information on key market drivers, restraints, challenges, and opportunities.

The report provides insights into the following pointers:

-□Analysis of key drivers (Increasing frequency and sophistication of cyberattacks, Growing BYOD trend necessitating network security measures, Rising cloud adoption and remote work trend), restraints (High implementation costs, Shortage of skilled cybersecurity professionals), opportunities (Simplified management and enhanced protection achieved using secure access service edge framework, Implementation of zero-trust approach in network security), and challenges (Lack of awareness and training concerning network security technologies, Integration complexities)

-□Product Development/Innovation: Detailed insights on upcoming technologies, research & development activities, and new product & service launches in the network security market

-□Market Development: Comprehensive information about lucrative markets - the report analyses the network security market across varied regions

-□Market Diversification: Exhaustive information about new products & services, untapped geographies, recent developments, and investments in the network security market

-□Competitive Assessment: In-depth assessment of market shares, growth strategies, and service offerings of leading players in the network security market, including Palo Alto Networks (US), Cisco (US), CrowdStrike (US), Check Point (Israel), and Trend Micro (Japan)

Table of Contents:

Network Security Market By Solution (Firewall/Next Generation Firewall, Secure Web Gateways, Unified Threat Management, Network Detection & Response, Network Access Control), Network Environment (Branch, Campus, Data Center)- Global Forecast to 2030

Market Report | 2025-12-05 | 465 pages | MarketsandMarkets

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	$4950.00
	Multi User	$6650.00
	Corporate License	$8150.00
	Enterprise Site License	$10000.00
	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	2026-02-11
		Signature	