+357 96 030922
info@marketpublishers.com

Next Generation Firewall Market ? Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution & Service), By Enterprise Size (Small & Medium Enterprise (SME) & Large Enterprise), By End Use Industry (BFSI; IT & Telecom; Retail; Defense; Healthcare; Education & Others), By Region & Competition, 2021-2031F

https://marketpublishers.com/r/NE16C3D60894EN.html
Date: January 2026
Pages: 185
Price: US$ 4,500.00 (Single User License)
ID: NE16C3D60894EN

Abstracts

The Global Next Generation Firewall Market is projected to expand from USD 6.72 Billion in 2025 to USD 12.82 Billion by 2031, achieving a CAGR of 11.37%. A Next Generation Firewall (NGFW) is defined as a network security solution that combines traditional firewall functions with intrusion prevention, deep packet inspection, and application awareness to identify and block dynamic threats. The market is largely driven by the rising frequency of cyber incursions and the requirement for unified security across cloud and hybrid infrastructures, a demand further intensified by strict regulatory compliance mandates calling for detailed network visibility. According to ISACA, 55% of survey respondents in 2024 reported an increase in attack volume, highlighting the essential need for the robust defense mechanisms provided by NGFWs.

However, market growth is significantly hindered by the operational complexity of these systems and a critical shortage of qualified personnel. Organizations often face difficulties in effectively configuring and maintaining these platforms due to a lack of internal expertise, which creates a barrier to adoption for resource-limited enterprises. According to ISC2, the global cybersecurity workforce gap was estimated at 4.8 million professionals in 2024, a disparity that severely restricts the successful deployment and management of network security technologies.

Market Driver

The increasing sophistication of cyber threats and advanced persistent threats acts as a primary catalyst for the Global Next Generation Firewall Market. Modern adversaries are frequently using complex encryption to hide malware, rendering traditional firewalls ineffective and necessitating the deep packet inspection capabilities of Next Generation Firewalls. This trend is emphasized by a surge in attacks aimed at bypassing perimeter defenses via encrypted channels; according to SonicWall?s '2024 Mid-Year Cyber Threat Report' from July 2024, encrypted threats increased by 92% during the analyzed period. Additionally, Check Point reported that global cyber attacks rose by 30% year-over-year in the second quarter of 2024, creating an urgent imperative for the robust protection offered by modern NGFW solutions.

The integration of AI and machine learning for automated threat detection represents a second transformative driver, allowing firewalls to neutralize zero-day exploits in real time. As network environments become more complex, enterprises are adopting AI-driven NGFWs to improve operational efficiency and reduce the heavy financial burden associated with incident response. This technological evolution creates significant value by minimizing breach costs through rapid containment and predictive analytics. According to IBM?s 'Cost of a Data Breach Report 2024' from July 2024, organizations that extensively deployed security AI and automation incurred average breach costs that were USD 1.88 million lower than those without these capabilities, making automated remediation a decisive factor in procurement strategies.

Market Challenge

The operational complexity of Next Generation Firewalls, combined with a persistent shortage of skilled professionals, presents a significant restraint on market growth. Organizations frequently struggle to configure and manage these security solutions effectively, as the advanced features require specialized technical knowledge that is often unavailable internally. This capability gap discourages enterprises from investing in comprehensive network security platforms, as they cannot guarantee proper deployment or ongoing maintenance. When companies lack the internal expertise to manage granular policies and deep packet inspection, they often defer upgrades or opt for less demanding security alternatives.

Consequently, the inability to fully utilize the functionalities of these systems leads to delayed procurement cycles and reduced adoption rates. The reliance on scarce talent creates a bottleneck where security strategies are compromised by resource limitations rather than technological capability. According to the World Economic Forum, 52% of organizations in 2024 identified a lack of resources and skills as their primary challenge when designing for cyber resilience. This deficit directly impacts the market by limiting the addressable customer base to those with sufficient operational maturity to handle these complex environments.

Market Trends

The convergence of Next-Generation Firewalls with SASE architectures is reshaping the market as enterprises move toward unified platforms. This trend involves integrating SD-WAN and firewall capabilities into cloud-delivered services to ensure consistent policy enforcement across distributed locations. Vendors are bundling these functions to eliminate the fragmentation caused by disparate point solutions, effectively reducing administrative burdens. This architectural shift is gaining traction as organizations prioritize seamless security integration over isolated appliances; according to Cisco?s '2024 Global Networking Trends Report' from May 2024, 76% of organizations plan to adopt a Secure Access Service Edge (SASE) architecture that integrates SD-WAN and cloud security within the next two years.

Simultaneously, the expansion of capabilities for IoT and OT security is a critical focal point for vendors addressing vulnerable industrial environments. As operational technology converges with IT networks, legacy systems are exposed to external attacks, necessitating firewalls with specialized protocols. Manufacturers are embedding granular discovery and segmentation tools directly into appliances to prevent lateral movement from compromised machinery. The urgency of this development is driven by the high rate of breaches targeting these sectors; according to Fortinet?s '2024 State of Operational Technology and Cybersecurity Report' from June 2024, 73% of organizations experienced an intrusion that impacted OT systems or both IT and OT environments in the prior year, highlighting the need for expanded defenses.

Key Market Players

Palo Alto Networks, Inc.

Fortinet, Inc.

Check Point Software Technologies Ltd.

Cisco Systems, Inc.

Juniper Networks, Inc.

Sophos Ltd.

Barracuda Networks, Inc.

SonicWall Inc.

Huawei Technologies Co., Ltd.

Stormshield SAS

Report Scope

In this report, the Global Next Generation Firewall Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Next Generation Firewall Market, By Component

Solution & Service

Next Generation Firewall Market, By Enterprise Size

Small & Medium Enterprise (SME) & Large Enterprise

Next Generation Firewall Market, By End Use Industry

BFSI; IT & Telecom; Retail; Defense; Healthcare; Education & Others

Next Generation Firewall Market, By Region

North America

United States

Canada

+357 96 030922
info@marketpublishers.com

- Mexico
- Europe
  - France
  - United Kingdom
  - Italy
  - Germany
  - Spain
- Asia Pacific
  - China
  - India
  - Japan
  - Australia
  - South Korea
- South America
  - Brazil
  - Argentina
  - Colombia
- Middle East & Africa
  - South Africa

Saudi Arabia

UAE

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Next Generation Firewall Market.

Available Customizations:

Global Next Generation Firewall Market report with the given market data, TechSci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

+357 96 030922
info@marketpublishers.com

Contents

6. NORTH AMERICA NEXT GENERATION FIREWALL MARKET OUTLOOK

7. EUROPE NEXT GENERATION FIREWALL MARKET OUTLOOK

8. ASIA PACIFIC NEXT GENERATION FIREWALL MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

Market Publishers

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Next Generation Firewall Market ? Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution & Service), By Enterprise Size (Small & Medium Enterprise (SME) & Large Enterprise), By End Use Industry (BFSI; IT & Telecom; Retail; Defense; Healthcare; Education & Others), By Region & Competition, 2021-2031F

Product link: https://marketpublishers.com/r/NE16C3D60894EN.html

Price: US$ 4,500.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/NE16C3D60894EN.html