Network Security Market Report by Component (Solutions, Services), Deployment Mode (Cloud-based, On-premises), Organization Size (Large Enterprises, Small and Medium-sized Enterprises), Industry Vertical (IT and Telecommunication, BFSI, Aerospace and Defense, Government, Healthcare, Retail, Manufacturing, Energy and Utilities, and Others), and Region 2024-2032

Market Report | 2024-03-02 | 145 pages | IMARC Group

AVAILABLE LICENSES:

- Electronic (PDF) Single User $3899.00
- Five User Licence $4899.00
- Enterprisewide License $5899.00

Report description:

The global network security market size reached US$ 35.4 Billion in 2023. Looking forward, IMARC Group expects the market to reach US$ 125.8 Billion by 2032, exhibiting a growth rate (CAGR) of 14.9% during 2024-2032. The growing incidences of cyber threats and data breaches, rising adoption of the Internet of Things (IoT) devices, and stringent data protection regulations and compliance standards are some of the major factors propelling the market.

Network security refers to the practice of safeguarding computer networks and data from unauthorized access, attacks, and potential disruptions. It comprises a wide range of measures, such as deploying firewalls, intrusion detection systems, encryption protocols, and access controls, that are designed to protect the integrity, confidentiality, and availability of network resources. It assists in preventing unauthorized users from gaining access to sensitive information or causing network breaches. As it aids in identifying and mitigating potential threats, the demand for network security is increasing around the world.

At present, the rising need to safeguard sensitive information from misuse and prevent financial losses is contributing to the growth of the market. In line with this, the increasing adoption of network security among business organizations to ensure the reliability and safety of their digital infrastructure and mitigate the risks associated with cyberattacks and data breaches is strengthening the growth of the market. Moreover, the growing demand for network security in various sectors to maintain the trust of the clients is positively influencing the market. In addition, the rising popularity of bring-your-own-device (BYOD) in

organizations across the globe is offering lucrative growth opportunities to industry investors. Furthermore, the increasing number of online financial transactions worldwide is supporting the growth of the market. Besides this, the rising adoption of fifth generation (5G) technology is bolstering the growth of the market.

Network Security Market Trends/Drivers:
Rising incidences of cyber threats and data breaches

Cyber threats comprise a wide range of malicious activities, such as hacking, phishing, malware attacks, and ransomware incidents. These threats exploit vulnerabilities in networks, systems, and software to gain unauthorized access, steal sensitive information, or disrupt operations. In line with this, business organizations are seeking security solutions that assist in safeguarding their networks and preventing financial loss, reputational damage, and legal repercussions. As a result, they are investing in advanced intrusion detection systems, next-gen firewalls, and threat intelligence solutions to proactively identify and thwart potential threats. Furthermore, the rising demand for network security due to the increasing incidences of cyber threats and data breaches is contributing to the growth of the market.

Increasing adoption of the Internet of Things (IoT) devices

The rising adoption of the Internet of Things (IoT) devices, along with the increasing popularity of cloud computing, is bolstering the growth of the market. IoT devices offer enhanced convenience and efficiency and allow users to remotely control devices, gather real-time data, and automate processes. In addition, the rapid expansion of IoT devices is transforming the way data is stored, accessed, and transmitted. Besides this, organizations are investing in comprehensive security solutions, such as encryption protocols, identity and access management, and secure communication channels, that can secure data in transit and at rest across diverse platforms.

Stringent data protection regulations

Stringent data protection regulations are legal frameworks that are designed to ensure the privacy and security of personal and sensitive information in the digital world. Such regulations grant individuals greater control over their personal data and require organizations to obtain explicit consent for data collection, provide transparent privacy policies, and offer mechanisms for data access and erasure. Moreover, various stringent data protection regulations and compliance standards, such as General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA), are compelling organizations to prioritize security solutions. Non-compliance with these regulations can result in substantial fines and damage to the reputation of a company. Businesses are adopting advanced security solutions that enable them to maintain data privacy and mitigate these risks.

Network Security Industry Segmentation:
IMARC Group provides an analysis of the key trends in each segment of the global network security market report, along with forecasts at the global, regional and country levels from 2024-2032. Our report has categorized the market based on component, deployment mode, organization size and industry vertical.

Breakup by Component:

Solutions
Firewalls
Antivirus/Antimalware
Network Access Control (NAC)
Data Loss Prevention

IDS/IPS
Secure Web Gateways
DDoS Mitigation
Unified Threat Management
Others
Services
Professional Services
Managed Services

Solutions represent the largest market segment

The report has provided a detailed breakup and analysis of the market based on the component. This includes solutions (firewalls, antivirus or antimalware, network access control (NAC), data loss prevention, IDS or IPS, secure web gateways, DDoS mitigation, unified threat management, and others) and services (professional services and managed services). According to the report, solutions (firewalls) represented the largest segment.

Network security solutions, such as firewalls, play a vital role in safeguarding digital environments from unauthorized access and cyber threats. Firewalls act as protective barriers that monitor incoming and outgoing network traffic and analyze data packets and determine whether they should be allowed or blocked based on predefined security rules. They serve as the first line of defense against unauthorized access, malware, and other malicious activities. Modern firewalls often employ advanced techniques, such as deep packet inspection, intrusion detection, and application filtering, to provide comprehensive security.

Breakup by Deployment Mode:

Cloud-based
On-premises

Cloud based accounts for the majority of the market share

The report has provided a detailed breakup and analysis of the market based on the deployment mode. This includes cloud-based and on-premises. According to the report, cloud-based represented the largest segment.

Cloud-based deployment involves the utilization of security solutions that are hosted and operated in cloud environments. This approach offers several advantages, such as enhanced scalability, flexibility, and reduced infrastructure costs. Organizations can leverage cloud-based security solutions to protect their data and network resources without the need for extensive on-premises hardware and maintenance. In addition, they provide real-time threat detection and response and ensure that data remains secure even as it travels between on-premises locations and cloud platforms. The scalability of cloud-based deployments allows businesses to adjust their security measures according to their needs.

Breakup by Organization Size:

Large Enterprises
Small and Medium-sized Enterprises

The report has provided a detailed breakup and analysis of the market based on the organization size. This includes large enterprises and small and medium-sized enterprises.

Large enterprises often deal with a higher volume of data and face more cyber threats due to their visibility and prominence. In addition, they invest in comprehensive security solutions that include advanced firewalls, intrusion detection systems, threat intelligence, and security information and event management (SIEM) tools. Their security strategies focus on protecting critical assets, adhering to compliance standards, and maintaining robust incident response capabilities.

Small and medium-sized enterprises (SMEs) have fewer resources than large enterprises. Network security solutions for SMEs are tailored to their needs and offer affordable and effective protection. These solutions generally include firewall appliances, anti-malware tools, and cloud-based security services. Additionally, SMEs prioritize user-friendly interfaces and centralized management to streamline security operations, which is positively influencing the market.

Breakup by Industry Vertical:

IT and Telecommunication
BFSI
Aerospace and Defense
Government
Healthcare
Retail
Manufacturing
Energy and Utilities
Others

IT and telecommunication hold the biggest market share

The report has provided a detailed breakup and analysis of the market based on the industry vertical. This includes IT and telecommunication, BFSI, aerospace and defense, government, healthcare, retail, manufacturing, energy and utilities, and others. According to the report, IT and telecommunication represented the largest segment.

In the IT and telecommunications industry, network security plays a crucial role due to its inherent reliance on data exchange and communication. Robust security solutions are essential to safeguard sensitive information, maintain service availability, and prevent cyber threats. The emergence of digital services, cloud computing, and IoT devices has expanded the attack surface, which makes them prime targets for cybercriminals. As a result, these organizations invest in various security solutions, such as intrusion detection systems, encryption technologies, and vulnerability assessment tools, to secure the transmission of data and protect customer information.

Breakup by Region:

North America
United States
Canada
Asia-Pacific
China
Japan
India
South Korea
Australia
Indonesia

Others
Europe
Germany
France
United Kingdom
Italy
Spain
Russia
Others
Latin America
Brazil
Mexico
Others
Middle East and Africa

North America exhibits a clear dominance, accounting for the largest network security market share

The report has also provided a comprehensive analysis of all the major regional markets, which include North America (the United States and Canada); Asia Pacific (China, Japan, India, South Korea, Australia, Indonesia, and others); Europe (Germany, France, the United Kingdom, Italy, Spain, Russia, and others); Latin America (Brazil, Mexico, and others); and the Middle East and Africa. According to the report, North America accounted for the largest market share.

North America held the biggest market share due to the improved technological infrastructure. Apart from this, the rising adoption of cloud computing and digital services is contributing to the growth of the market in the region. In line with this, the presence of well-established cybersecurity companies is propelling the growth of the market. Besides this, the rising focus on avoiding legal consequences and reputational damage is bolstering the growth of the market in the North America region.

Competitive Landscape:
Various manufacturers are investing in research and development (R&D) activities to create innovative solutions that can adapt to emerging threats. This involves leveraging technologies, such as artificial intelligence (AI), machine learning (ML), and behavioral analytics, to detect and mitigate advanced and previously unseen cyber threats. In line with this, many companies are focusing on enhancing their threat intelligence capabilities. They are gathering and analyzing data from various sources to identify patterns and indicators of potential cyberattacks that allow organizations to detect threats early and respond effectively. Apart from this, key players are developing specialized solutions for cloud security, which involves securing data in transit and at rest, protecting cloud infrastructure, and providing visibility into cloud-related threats.

The report has provided a comprehensive analysis of the competitive landscape in the market. Detailed profiles of all major companies have also been provided. Some of the key players in the market include:

AT&T Inc.
Avast Software s.r.o.
Broadcom Inc.
Cisco Systems Inc.
Fortinet Inc.
International Business Machines Corporation
Juniper Networks Inc.
NortonLifeLock Inc.

Palo Alto Networks Inc.
SonicWall
Trellix (Symphony Technology Group)
Trend Micro Incorporated

Recent Developments:
In November 2022, Cisco and Red Hat collaborated to accelerate deployment and simplify management. The companies integrated Cisco?s cloud-operations management platform, Intersight, and Red Hat OpenShift Assisted Installer, which controls OpenShift clusters, to handle the complex and time-consuming process of networking in a containerized environment.
In April 2023, Trellix, the cybersecurity company announced the launch of Trellix Endpoint Security Suite. Trellix Endpoint Security Suite's products and advanced capabilities empower Security Operations Center (SOC) analysts with superior visibility and control in a single pane of glass to proactively secure all endpoints.
In 2023, Fortinet, the global cybersecurity leader driving the convergence of networking and security, announced that Emirates National Oil Company Limited (ENOC), a wholly owned company of the Government of Dubai, has chosen Fortinet Secure SD-wide area network (WAN) to transform customer experience and increase operational efficiency.

Key Questions Answered in This Report

1. What was the size of the global network security market in 2023?
2. What is the expected growth rate of the global network security market during 2024-2032?
3. What are the key factors driving the global network security market?
4. What has been the impact of COVID-19 on the global network security market?
5. What is the breakup of the global network security market based on the component?
6. What is the breakup of the global network security market based on the deployment mode?
7. What is the breakup of the global network security market based on end user?
8. What are the key regions in the global network security market?
9. Who are the key players/companies in the global network security market?

Table of Contents:

1 Preface
2 Scope and Methodology
2.1 Objectives of the Study
2.2 Stakeholders
2.3 Data Sources
2.3.1 Primary Sources
2.3.2 Secondary Sources
2.4 Market Estimation
2.4.1 Bottom-Up Approach
2.4.2 Top-Down Approach
2.5 Forecasting Methodology
3 Executive Summary
4 Introduction
4.1 Overview
4.2 Key Industry Trends
5 Global Network Security Market
5.1 Market Overview
5.2 Market Performance

5.3 Impact of COVID-19
5.4 Market Forecast
6 Market Breakup by Component
6.1 Solutions
6.1.1 Market Trends
6.1.2 Key Segments
6.1.2.1 Firewalls
6.1.2.2 Antivirus/Antimalware
6.1.2.3 Network Access Control (NAC)
6.1.2.4 Data Loss Prevention
6.1.2.5 IDS/IPS
6.1.2.6 Secure Web Gateways
6.1.2.7 DDoS Mitigation
6.1.2.8 Unified Threat Management
6.1.2.9 Others
6.1.3 Market Forecast
6.2 Services
6.2.1 Market Trends
6.2.2 Key Segments
6.2.2.1 Professional Services
6.2.2.2 Managed Services
6.2.3 Market Forecast
7 Market Breakup by Deployment Mode
7.1 Cloud-based
7.1.1 Market Trends
7.1.2 Market Forecast
7.2 On-premises
7.2.1 Market Trends
7.2.2 Market Forecast
8 Market Breakup by Organization Size
8.1 Large Enterprises
8.1.1 Market Trends
8.1.2 Market Forecast
8.2 Small and Medium-sized Enterprises
8.2.1 Market Trends
8.2.2 Market Forecast
9 Market Breakup by Industry Vertical
9.1 IT and Telecommunication
9.1.1 Market Trends
9.1.2 Market Forecast
9.2 BFSI
9.2.1 Market Trends
9.2.2 Market Forecast
9.3 Aerospace and Defense
9.3.1 Market Trends
9.3.2 Market Forecast
9.4 Government

9.4.1 Market Trends
9.4.2 Market Forecast
9.5 Healthcare
9.5.1 Market Trends
9.5.2 Market Forecast
9.6 Retail
9.6.1 Market Trends
9.6.2 Market Forecast
9.7 Manufacturing
9.7.1 Market Trends
9.7.2 Market Forecast
9.8 Energy and Utilities
9.8.1 Market Trends
9.8.2 Market Forecast
9.9 Others
9.9.1 Market Trends
9.9.2 Market Forecast
10 Market Breakup by Region
10.1 North America
10.1.1 United States
10.1.1.1 Market Trends
10.1.1.2 Market Forecast
10.1.2 Canada
10.1.2.1 Market Trends
10.1.2.2 Market Forecast
10.2 Asia-Pacific
10.2.1 China
10.2.1.1 Market Trends
10.2.1.2 Market Forecast
10.2.2 Japan
10.2.2.1 Market Trends
10.2.2.2 Market Forecast
10.2.3 India
10.2.3.1 Market Trends
10.2.3.2 Market Forecast
10.2.4 South Korea
10.2.4.1 Market Trends
10.2.4.2 Market Forecast
10.2.5 Australia
10.2.5.1 Market Trends
10.2.5.2 Market Forecast
10.2.6 Indonesia
10.2.6.1 Market Trends
10.2.6.2 Market Forecast
10.2.7 Others
10.2.7.1 Market Trends
10.2.7.2 Market Forecast

10.3 Europe
10.3.1 Germany
10.3.1.1 Market Trends
10.3.1.2 Market Forecast
10.3.2 France
10.3.2.1 Market Trends
10.3.2.2 Market Forecast
10.3.3 United Kingdom
10.3.3.1 Market Trends
10.3.3.2 Market Forecast
10.3.4 Italy
10.3.4.1 Market Trends
10.3.4.2 Market Forecast
10.3.5 Spain
10.3.5.1 Market Trends
10.3.5.2 Market Forecast
10.3.6 Russia
10.3.6.1 Market Trends
10.3.6.2 Market Forecast
10.3.7 Others
10.3.7.1 Market Trends
10.3.7.2 Market Forecast
10.4 Latin America
10.4.1 Brazil
10.4.1.1 Market Trends
10.4.1.2 Market Forecast
10.4.2 Mexico
10.4.2.1 Market Trends
10.4.2.2 Market Forecast
10.4.3 Others
10.4.3.1 Market Trends
10.4.3.2 Market Forecast
10.5 Middle East and Africa
10.5.1 Market Trends
10.5.2 Market Breakup by Country
10.5.3 Market Forecast
11 SWOT Analysis
11.1 Overview
11.2 Strengths
11.3 Weaknesses
11.4 Opportunities
11.5 Threats
12 Value Chain Analysis
13 Porters Five Forces Analysis
13.1 Overview
13.2 Bargaining Power of Buyers
13.3 Bargaining Power of Suppliers

13.4 Degree of Competition
13.5 Threat of New Entrants
13.6 Threat of Substitutes
14 Price Analysis
15 Competitive Landscape
15.1 Market Structure
15.2 Key Players
15.3 Profiles of Key Players
15.3.1 AT&T Inc.
15.3.1.1 Company Overview
15.3.1.2 Product Portfolio
15.3.1.3 Financials
15.3.1.4 SWOT Analysis
15.3.2 Avast Software s.r.o.
15.3.2.1 Company Overview
15.3.2.2 Product Portfolio
15.3.2.3 Financials
15.3.3 Broadcom Inc.
15.3.3.1 Company Overview
15.3.3.2 Product Portfolio
15.3.3.3 Financials
15.3.3.4 SWOT Analysis
15.3.4 Cisco Systems Inc.
15.3.4.1 Company Overview
15.3.4.2 Product Portfolio
15.3.4.3 Financials
15.3.4.4 SWOT Analysis
15.3.5 Fortinet Inc.
15.3.5.1 Company Overview
15.3.5.2 Product Portfolio
15.3.5.3 Financials
15.3.5.4 SWOT Analysis
15.3.6 International Business Machines Corporation
15.3.6.1 Company Overview
15.3.6.2 Product Portfolio
15.3.6.3 Financials
15.3.6.4 SWOT Analysis
15.3.7 Juniper Networks Inc.
15.3.7.1 Company Overview
15.3.7.2 Product Portfolio
15.3.7.3 Financials
15.3.7.4 SWOT Analysis
15.3.8 NortonLifeLock Inc.
15.3.8.1 Company Overview
15.3.8.2 Product Portfolio
15.3.8.3 Financials
15.3.8.4 SWOT Analysis

15.3.9 Palo Alto Networks Inc.
15.3.9.1 Company Overview
15.3.9.2 Product Portfolio
15.3.9.3 Financials
15.3.9.4 SWOT Analysis
15.3.10 SonicWall
15.3.10.1 Company Overview
15.3.10.2 Product Portfolio
15.3.11 Trellix (Symphony Technology Group)
15.3.11.1 Company Overview
15.3.11.2 Product Portfolio
15.3.12 Trend Micro Incorporated
15.3.12.1 Company Overview
15.3.12.2 Product Portfolio
15.3.12.3 Financials
15.3.12.4 SWOT Analysis

Network Security Market Report by Component (Solutions, Services), Deployment Mode (Cloud-based, On-premises), Organization Size (Large Enterprises, Small and Medium-sized Enterprises), Industry Vertical (IT and Telecommunication, BFSI, Aerospace and Defense, Government, Healthcare, Retail, Manufacturing, Energy and Utilities, and Others), and Region 2024-2032

Market Report | 2024-03-02 | 145 pages | IMARC Group

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
	Electronic (PDF) Single User	$3899.00
	Five User Licence	$4899.00
	Enterprisewide License	$5899.00
	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	2025-05-07
		Signature	