+44 20 8123 2220
info@marketpublishers.com

Wireless Network Security Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented by Deployment Model (Cloud, On-premise), By Security Type (Encryption, Authentication, Intrusion Detection and Prevention Systems (IDPS), Firewalls), By End-User Industry (Consumer, IT and Telecom, Healthcare, Banking, Financial Services, and Insurance (BFSI), Government and Defense, Others), By Region, By Competition, 2018-2028

https://marketpublishers.com/r/WCAA3F5CC2D1EN.html
Date: October 2023
Pages: 181
Price: US$ 4,900.00 (Single User License)
ID: WCAA3F5CC2D1EN

Abstracts

Global Wireless Network Security Market has experienced tremendous growth in recent years and is poised to continue its strong expansion. The Wireless Network Security Market reached a value of USD 20.65 billion in 2022 and is projected to maintain a compound annual growth rate of 13.76% through 2028.

The Global Wireless Network Security market continues to grow as organizations increasingly leverage emerging technologies to empower their workforce and secure their networks. Wireless network providers are offering talent management platforms that provide unprecedented visibility into employee performance and productivity using wearable devices and behavioral analytics.

Tools like augmented and virtual reality headsets allow companies to monitor behaviors and detect anomalies in real-time when worn by employees. This helps address challenges around fraud prevention, regulatory compliance and cybersecurity risk for

+44 20 8123 2220
info@marketpublishers.com

financial institutions and other organizations. As remote and hybrid work models become more common, these data-driven insights from wearable devices are critical for effective oversight of global operations.

Major companies are utilizing mixed reality and sensor data from wearables to streamline collaboration between distributed teams. This enables more effective engagement with remote employees and digital customers. Wireless network security vendors are also investing heavily in predictive modeling and artificial intelligence integration with these devices.

By analyzing behavioral patterns and sensor data using AI, wireless network providers can help predict and prevent security threats. Applications that leverage wearable data like predictive maintenance, optimized decision making and personalized digital services for customers are well-positioned to grow. Overall, the outlook for the global wireless network security market remains strong as wearables continue to integrate new AI capabilities that address the evolving needs of the digital workplace.

Key Market Drivers

Increasing Adoption of BYOD and CYOD Trends

The adoption of bring your own device (BYOD) and choose your own device (CYOD) trends in organizations has increased manifold in recent years. This has led to a surge in the number of personal devices being connected to organizational networks. However, these devices often lack adequate security measures leaving the networks vulnerable to threats. With critical data now accessible over these devices, companies are investing heavily in wireless network security solutions to protect their networks and data from unauthorized access and cyberattacks. The need to secure these devices and the data they access is a major driver boosting spending on wireless intrusion prevention systems, VPNs, firewalls and other network security solutions.

Rising Threat of Cybercrimes and Data Breaches

As organizations increasingly rely on wireless networks and mobile devices, the threat of cybercrimes and data breaches has heightened significantly. Cybercriminals are exploiting vulnerabilities in wireless networks and launching sophisticated attacks such as man-in-the-middle, denial-of-service, and evil twin to steal sensitive data. The monetary and reputational losses incurred due to data breaches have pushed companies to bolster their wireless security posture. They are implementing robust

authentication, encryption, intrusion detection, and other advanced solutions to safeguard wireless networks, endpoints, and the data transmitted over them. This growing threat perception is fueling demand in the global wireless network security market.

Stringent Regulatory Standards and Compliance Requirements

Regulatory bodies around the world have introduced stringent data privacy and security laws to protect organizational and personal data from misuse and cyberattacks. Non-compliance with these regulations can attract heavy financial penalties. For instance, General Data Protection Regulation (GDPR) in Europe and California Consumer Privacy Act (CCPA) in the US mandate how companies collect, store, and use personal information. Similarly, the Payment Card Industry Data Security Standard (PCI DSS) has strict wireless network security guidelines for companies dealing with credit card transactions. To adhere to these compliance standards, businesses are compelled to invest in advanced wireless security controls which is boosting market revenues.

Key Market Challenges

Managing Increasingly Sophisticated Threat Landscape

As wireless networks become more ubiquitous and valuable assets for both consumers and businesses, the threat landscape continues to evolve rapidly as well. Hackers and cybercriminals are developing increasingly sophisticated techniques such as zero-day exploits, advanced persistent threats, ransomware, and distributed denial of service attacks to infiltrate networks and steal sensitive data. Keeping pace with these evolving threats presents a major challenge for wireless network security vendors and customers alike. Solutions must not only protect against current known threats, but also predict and prevent future threats that have yet to emerge. This requires significant investment in research and development to stay ahead of malicious actors. Additionally, security controls need to be updated frequently through patches and new releases to close vulnerabilities as they are discovered. For network operators, this ongoing maintenance and upgrade process can be costly and disrupt business operations if not implemented carefully. Overall, the escalating sophistication of cyber threats will continue testing the innovation and agility of wireless network security providers worldwide.

Ensuring Privacy and Compliance with Regulations

With wireless networks carrying more and more sensitive data, privacy and compliance

+44 20 8123 2220
info@marketpublishers.com

with regulations have become heightened priorities. However, ensuring privacy and meeting all applicable compliance standards is challenging given the complexity of today's networks and evolving legal/regulatory landscape. Wireless carriers and enterprises must have visibility into all network activity in order to detect threats, but this visibility can also enable unauthorized access to private data if not properly safeguarded and anonymized. At the same time, a growing number of jurisdictions have implemented stringent privacy laws like the California Consumer Privacy Act (CCPA) and Europe's General Data Protection Regulation (GDPR) that impose hefty fines for non-compliance. Network operators are under pressure to not only protect customer privacy, but also meticulously document and audit their privacy practices. Additionally, certain sectors like healthcare, financial services and government have their own industry-specific compliance rules to consider. Navigating this maze of global privacy regulations and standards is a major undertaking that will continue to challenge wireless network security vendors and users..

Key Market Trends

Increasing Adoption of Cloud-Based Security Solutions

The adoption of cloud-based security solutions is growing significantly across organizations as they offer advantages like scalability, cost-effectiveness and centralized management over on-premise solutions. Cloud-based WLAN security solutions automate security tasks, enable easy configuration of multiple access points from a single console and provide visibility into the entire wireless network. They also offer advanced features like integrated next-generation firewalls, application control and URL filtering. With work from home becoming common, cloud-based solutions have gained more prominence as employees can securely access corporate resources remotely. Their ability to adapt security policies according to the network usage and detect as well as prevent threats in real-time is driving greater acceptance. It is estimated that the market for cloud-based WLAN security will grow at over 15% annually in the coming years as businesses recognize the benefits of the cloud model for wireless network protection.

Rising Importance of AI and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) technologies are revolutionizing the wireless network security landscape by enabling cognitive capabilities. These technologies power solutions that can autonomously learn network behaviors, identify anomalies and threats, and respond to them quickly. For example, AI-powered Intrusion

+44 20 8123 2220
info@marketpublishers.com

Prevention Systems (IPS) can detect even the most sophisticated zero-day attacks by analyzing vast amounts of network traffic data. Similarly, ML-based solutions for wireless user and entity behavioral analytics (UEBA) can efficiently handle user access policies, detect insider threats, and automate change management by continuously learning patterns of approved behavior. As attacks become more advanced, AI/ML is playing a crucial role in augmenting security teams and keeping pace with the evolving threat landscape. It is projected that over 60% of WLAN vendors will integrate AI/ML in their product roadmaps by 2025 to deliver proactive protection, automated threat remediation and improved visibility for enterprises.

Increasing Focus on Encryption and Authentication

With the proliferation of IoT and BYOD trends, organizations are facing increased risks of unauthorized access and data theft over wireless networks. This has propelled a strong focus on robust encryption and multi-factor authentication techniques. Advanced Encryption Standard (AES) with 256-bit encryption and Wi-Fi Protected Access Version 3 (WPA3) are becoming baseline security standards for enterprise WLAN deployments. Meanwhile, 802.1X port-based network access control along with RADIUS server authentication provides a centralized way of controlling user access. Multi-factor authentication using a combination of username-password, one-time passwords, digital certificates and biometric identifiers is gaining traction to authenticate users and devices connecting over wireless networks. Stricter privacy laws have also necessitated deployment of encrypted VPN tunnels for remote access. Going forward, quantum-resistant algorithms, blockchain-based authentication and homomorphic encryption are expected to further strengthen wireless network protection in the coming years.

Segmental Insights

Deployment Model Insights

The cloud segment dominated the global wireless network security market in 2022 and is expected to maintain its dominance during the forecast period from 2022 to 2027. The cloud deployment model offers several benefits such as scalability, flexibility, and cost-effectiveness which has increased its adoption among organizations. Cloud wireless network security solutions can be easily scaled up or down based on the changing needs of organizations without incurring high upfront costs for hardware procurement. They also provide flexibility in terms of easy deployment and management of security solutions across distributed enterprise networks from any location. With the pay-as-you-go pricing model of cloud wireless network security, organizations only need to pay for

the resources they consume which helps reduce capital expenditure. These advantages have made cloud wireless network security solutions an attractive and affordable option for organizations of all sizes. Furthermore, the rise in remote and hybrid work culture amid the COVID-19 pandemic has accelerated the demand for cloud-based wireless security solutions to securely manage distributed workforce. As organizations continue to embrace digital transformation and cloud migration initiatives, the cloud segment is expected to continue dominating the global wireless network security market during the forecast period due to its compelling benefits over on-premise deployment.

Security Type Insights

Encryption dominated the global wireless network security market in 2022 and is expected to maintain its dominance during the forecast period. Encryption provides security to wireless networks by encoding data transmitted between wireless devices and access points so that it is protected and unintelligible to unauthorized parties who may attempt to intercept and eavesdrop on wireless transmissions. This is crucial as wireless networks are more vulnerable to security threats than wired networks due to the broadcast nature of the wireless signals and the lack of defined network perimeters. In 2022, the encryption segment accounted for the largest market share and this trend is expected to continue from 2023 to 2028. The widespread adoption of encryption standards such as WPA2/WPA3 for personal and enterprise Wi-Fi networks has propelled the encryption segment's growth. In addition, with the proliferation of IoT devices that connect to wireless networks, the need for encrypting data transmitted to and from these devices is increasing to prevent cyberattacks, thereby driving greater demand for encryption solutions in the coming years. Authentication, intrusion detection and prevention systems, and firewalls are other important types of wireless network security measures. However, encryption remains the most fundamental and widely used technique for securing wireless networks and maintaining privacy in an era of increased mobility and connectivity.

Regional Insights

North America dominated the global wireless network security market in 2022 and is expected to maintain its dominance during the forecast period from 2023 to 2030. The region accounted for over 35% share of the overall market revenue in 2022. This can be attributed to the early adoption of advanced technologies such as IoT, cloud computing, and BYOD across various industries in countries like the US and Canada. There has been a significant rise in the number of connected devices in North America which has increased the threat of cyber-attacks targeting these devices and networks. In order to

+44 20 8123 2220
info@marketpublishers.com

secure the wireless networks and connected devices from such threats, organizations in North America are increasingly investing in advanced wireless network security solutions such as WLAN security, wireless intrusion prevention system (WIPS), and secure sockets layer (SSL) VPNs. Furthermore, the presence of leading wireless network security vendors in the region is also supporting the market growth. Some of the major players operating in the North American wireless network security market are Cisco Systems, Juniper Networks, Fortinet, Motorola Solutions, and Sophos among others. With growing digitization and increasing number of connected devices, the need for robust wireless network security solutions will continue to rise in North America, allowing the region to retain its dominant position in the global market during the forecast period.

Key Market Players

Cisco Systems, Inc

Juniper Networks, Inc

Fortinet, Inc

Motorola Solutions, Inc

Sophos Group PLC

Aruba Networks, Inc

ARRIS Group, Inc.

Broadcom Inc

Extreme Networks, Inc

Ubiquiti Inc

Report Scope:

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

+44 20 8123 2220
info@marketpublishers.com

Wireless Network Security Market, By Deployment Model:

- Cloud
- On-premise

Wireless Network Security Market, By Security Type:

- Encryption
- Authentication
- Intrusion Detection and Prevention Systems (IDPS)
- Firewalls

Wireless Network Security Market, By End-User Industry:

- Consumer
- IT and Telecom
- Healthcare
- Banking, Financial Services, and Insurance (BFSI)
- Government and Defense

Wireless Network Security Market, By Region:

- North America
  - United States
  - Canada
  - Mexico
- Europe

+44 20 8123 2220
info@marketpublishers.com

- 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

+44 20 8123 2220
info@marketpublishers.com

Kuwait

Turkey

Egypt

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Wireless Network Security Market.

Available Customizations:

Global Wireless Network Security Market report with the given market data, Tech Sci 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).

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

7. NORTH AMERICA WIRELESS NETWORK SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

8. EUROPE WIRELESS NETWORK SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

9. ASIA-PACIFIC WIRELESS NETWORK SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

10. SOUTH AMERICA WIRELESS NETWORK SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

11. MIDDLE EAST AND AFRICA WIRELESS NETWORK SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

12. MARKET DYNAMICS

12.1. Drivers
12.2. Challenges

13. MARKET TRENDS & DEVELOPMENTS

14. COMPANY PROFILES

14.1. Cisco Systems, Inc
  14.1.1. Business Overview
  14.1.2. Key Revenue and Financials
  14.1.3. Recent Developments
  14.1.4. Key Personnel/Key Contact Person
  14.1.5. Key Product/Services Offered
14.2. Juniper Networks, Inc
  14.2.1. Business Overview
  14.2.2. Key Revenue and Financials
  14.2.3. Recent Developments
  14.2.4. Key Personnel/Key Contact Person
  14.2.5. Key Product/Services Offered
14.3. Fortinet, Inc
  14.3.1. Business Overview
  14.3.2. Key Revenue and Financials
  14.3.3. Recent Developments
  14.3.4. Key Personnel/Key Contact Person
  14.3.5. Key Product/Services Offered
14.4. Motorola Solutions, Inc
  14.4.1. Business Overview
  14.4.2. Key Revenue and Financials
  14.4.3. Recent Developments
  14.4.4. Key Personnel/Key Contact Person
  14.4.5. Key Product/Services Offered
14.5. Sophos Group PLC
  14.5.1. Business Overview
  14.5.2. Key Revenue and Financials
  14.5.3. Recent Developments
  14.5.4. Key Personnel/Key Contact Person

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Wireless Network Security Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented by Deployment Model (Cloud, On-premise), By Security Type (Encryption, Authentication, Intrusion Detection and Prevention Systems (IDPS), Firewalls), By End-User Industry (Consumer, IT and Telecom, Healthcare, Banking, Financial Services, and Insurance (BFSI), Government and Defense, Others), By Region, By Competition, 2018-2028

Product link: https://marketpublishers.com/r/WCAA3F5CC2D1EN.html

Price: US$ 4,900.00 (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/WCAA3F5CC2D1EN.html

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

**All fields are required

Custumer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms

+44 20 8123 2220
info@marketpublishers.com

& Conditions at https://marketpublishers.com/docs/terms.html

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970