

Enterprise Firewall Hardware Market - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Type of Deployment (On-premises, Cloud), By Organization (Small and Medium, Large), By End User (Healthcare, Manufacturing, Government, Retail, Education, Others), By Region, and By Competition, 2019-2029F

<https://marketpublishers.com/r/E0A4BE6BFF6CEN.html>

Date: May 2024

Pages: 180

Price: US\$ 4,900.00 (Single User License)

ID: E0A4BE6BFF6CEN

Abstracts

Global Enterprise Firewall Hardware Market was valued at USD 6.27 billion in 2023 and is anticipated to project robust growth in the forecast period with a CAGR of 8.81% through 2029. The Global Enterprise Firewall Hardware Market is experiencing strong growth driven by heightened cybersecurity priorities among organizations worldwide. In response to increasingly sophisticated cyber threats, the demand for advanced security solutions has surged. Enterprise firewalls stand as crucial safeguards, defending networks and systems against unauthorized access, malware, and cyberattacks. A growing number of organizations are adopting next-generation firewalls (NGFWs) with enhanced features like intrusion detection and prevention, deep packet inspection, and application-layer filtering. This market expansion is further fueled by the rapid evolution of the digital landscape, encompassing cloud computing and remote work, which necessitate scalable and adaptable firewall solutions. Moreover, compliance with stringent data protection regulations and the growing emphasis on cybersecurity best practices are driving the demand for enterprise firewalls. As businesses continue to prioritize robust cybersecurity strategies, the Global Enterprise Firewall Hardware Market is poised for sustained growth, playing a pivotal role in bolstering the digital defenses of organizations across various sectors.

Key Market Drivers

Rising Cybersecurity Concerns

The Global Enterprise Firewall Hardware Market is driven by the escalating concerns over cybersecurity in an increasingly digital-dependent world. With the proliferation of cyber threats, data breaches, and the growing value of digital assets, organizations are prioritizing robust cybersecurity measures. Enterprise firewalls have emerged as critical components of cybersecurity strategies, serving as the first line of defense against unauthorized access, malware, and other cyberattacks. The continuous evolution of cyber threats necessitates advanced firewall solutions, propelling the demand for next-generation firewalls (NGFWs) equipped with intrusion detection and prevention systems, deep packet inspection, and application-layer filtering. The ever-present need to safeguard sensitive data and protect against cyber threats positions the Global Enterprise Firewall Hardware Market for sustained growth as organizations fortify their digital defenses.

Expanding Digital Landscape

The rapid expansion of the digital landscape, including the adoption of cloud computing, remote work, and digital transformation initiatives, is a significant driver of the Global Enterprise Firewall Hardware Market. As businesses embrace digital technologies and migrate to cloud-based infrastructures, the need for scalable and adaptable firewall solutions becomes paramount. Enterprise firewalls are essential in securing data and network access across diverse environments, whether on-premises or in the cloud. The increasing reliance on remote work models and the integration of digital tools emphasize the importance of firewall solutions that can seamlessly protect data and systems in an evolving digital landscape.

Stringent Data Protection Regulations

Stringent data protection regulations, including GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and CCPA (California Consumer Privacy Act), are compelling organizations to invest in robust cybersecurity measures, driving the demand for enterprise firewall hardware. Compliance with these regulations mandates the implementation of comprehensive security measures to protect sensitive data and report data breaches promptly. Enterprise firewalls play a pivotal role in achieving compliance by safeguarding data integrity and preventing unauthorized access. As organizations strive to meet regulatory requirements and ensure data privacy, the Global Enterprise Firewall

Hardware Market witnesses sustained growth.

Increasing Awareness of Cybersecurity Best Practices

The growing awareness of cybersecurity best practices is fostering the adoption of enterprise firewalls. Organizations across industries are recognizing the significance of proactive cybersecurity measures to mitigate risks and protect their reputation. This awareness extends to the need for advanced firewall solutions that offer real-time threat detection, rapid response capabilities, and comprehensive network security. As cybersecurity best practices become integral to business operations, the demand for enterprise firewalls equipped with advanced features and capabilities continues to rise.

Integration of Advanced Security Features

Enterprise firewalls are evolving to address the dynamic threat landscape, with a growing focus on advanced security features. Organizations seek firewall solutions that offer not only traditional network security but also advanced capabilities such as behavior-based anomaly detection, sandboxing, and threat intelligence integration. The integration of artificial intelligence (AI) and machine learning (ML) algorithms enhances firewall performance by enabling proactive threat identification and response. As organizations prioritize the adoption of holistic security postures, enterprise firewalls are central to their cybersecurity strategies, spurring the market's growth.

Key Market Challenges

Diverse Firewall Ecosystem

The Global Enterprise Firewall Hardware Market faces a notable challenge due to the diversity of firewall solutions and providers available in the market. Organizations must navigate a complex landscape of firewall types, including traditional firewalls, next-generation firewalls (NGFWs), unified threat management (UTM) devices, and cloud-based firewall services. Each type offers varying features, capabilities, and deployment options. This diversity often leads to difficulties in selecting the most suitable firewall solution for specific organizational needs. Moreover, managing a heterogeneous firewall environment can be complex, requiring expertise and resources, which can pose challenges for organizations seeking consistent and effective network security.

Adaptation to Evolving Cyber Threats

The dynamic and evolving nature of cyber threats presents an ongoing challenge for the Global Enterprise Firewall Hardware Market. Cyberattack techniques and tactics continuously change, requiring firewall solutions to adapt and evolve rapidly to provide effective protection. Threat actors are increasingly sophisticated, employing tactics such as zero-day exploits, advanced persistent threats (APTs), and polymorphic malware. Firewall providers must stay ahead of these threats by incorporating advanced threat detection and prevention mechanisms into their solutions. Organizations relying on firewall protection face the challenge of keeping their security infrastructure up to date and adequately responding to emerging threats.

Complex Network Architectures

Modern organizations often employ complex network architectures that include hybrid cloud environments, multi-cloud deployments, remote workforces, and mobile devices. These diverse network configurations introduce complexities in firewall management and enforcement. Maintaining consistent security policies across on-premises, cloud, and remote environments can be challenging. Organizations must ensure that their firewall solutions are capable of securing these intricate network architectures while maintaining seamless connectivity and performance. This complexity can lead to operational challenges and the need for skilled personnel to manage and optimize firewall deployments.

Compliance and Regulatory Requirements

Compliance with various industry-specific regulations and data protection laws adds complexity to the Global Enterprise Firewall Hardware Market. Organizations operating in highly regulated sectors such as healthcare, finance, and government must adhere to stringent compliance requirements like HIPAA, PCI DSS, and GDPR. These regulations mandate specific security measures and data protection standards that firewall solutions must address. Ensuring firewall configurations align with these regulatory requirements can be demanding and necessitates continuous monitoring and adjustment. Non-compliance can result in legal consequences and reputational damage, making it a critical challenge for organizations to navigate within the firewall market.

Key Market Trends

Evolving Threat Landscape and Advanced Threat Detection

The Global Enterprise Firewall Hardware Market is witnessing a continuous evolution in response to the ever-changing threat landscape. Cyberattacks have become increasingly sophisticated, employing advanced techniques like zero-day exploits, ransomware, and targeted attacks. In response, firewall solutions are incorporating advanced threat detection and prevention capabilities. Next-generation firewalls (NGFWs) and unified threat management (UTM) devices are being equipped with intrusion detection and prevention systems (IDPS), sandboxing, and machine learning-based anomaly detection to proactively identify and mitigate emerging threats. This trend underscores the market's commitment to staying ahead of cyber adversaries and providing robust security solutions for organizations.

Cloud-native Firewall Solutions

The adoption of cloud-native firewall solutions is a notable trend in the Global Enterprise Firewall Hardware Market. As organizations migrate their applications and data to the cloud, there is a growing need for firewall solutions that can secure cloud environments effectively. Cloud-based firewall services offer scalable, on-demand security that aligns with the dynamic nature of cloud infrastructure. These solutions provide organizations with the flexibility to enforce consistent security policies across on-premises and cloud environments. Additionally, cloud-native firewall solutions often include features like application-level visibility, micro-segmentation, and automated scaling, enhancing their appeal to businesses undergoing digital transformation.

Zero-Trust Network Access (ZTNA)

The Zero-Trust Network Access (ZTNA) framework is gaining prominence within the enterprise firewall Hardware market. ZTNA is founded on the principle of 'never trust, always verify,' which means that users and devices are not granted implicit trust, even if they are inside the corporate network. This security model is becoming increasingly essential as organizations adopt remote work and hybrid work models. ZTNA solutions, often integrated with firewalls, enforce strict access controls based on user identity, device posture, and contextual factors. This approach enhances security by reducing the attack surface and minimizing lateral movement by threat actors. As organizations prioritize ZTNA to bolster their security posture, firewall providers are incorporating ZTNA capabilities into their offerings to meet this growing demand.

Integrated Security and Convergence

The convergence of security functions within firewalls is a prevailing trend in the enterprise firewall hardware market. Organizations seek integrated security solutions that streamline security management and reduce complexity. Firewall vendors are responding by incorporating additional security features, such as intrusion prevention, antivirus, web filtering, and secure web gateways, into their firewall appliances. This consolidation of security functions within a single device or platform provides organizations with comprehensive threat protection and simplifies security administration. As businesses look for holistic security solutions that address a wide range of threats, the trend of integrated security within firewalls continues to gain momentum.

Segmental Insights

Type of Deployment Insights

The cloud deployment segment dominated the Global Enterprise Firewall Hardware Market, and this dominance is expected to persist throughout the forecast period. The shift towards cloud-based solutions is significantly driving this market forward. Internationally, businesses are increasingly opting for cloud-native firewall solutions to protect their data and applications housed in cloud environments. The adaptability, scalability, and cost-effectiveness of these cloud-based firewalls closely align with changing business needs. With the rise in remote work, digital transformation, and the widespread use of cloud infrastructure, enterprises are depending on cloud-deployed firewalls to ensure seamless security across both on-premises and cloud setups. Additionally, cloud-native firewall solutions often offer advanced functionalities such as application-level visibility, micro-segmentation, and automated scaling, making them even more appealing. Furthermore, the Zero Trust Network Access (ZTNA) framework, which emphasizes stringent access controls and user authentication, is gaining traction in today's security landscape. Cloud-based firewall solutions are particularly well-suited for implementing ZTNA, further driving their adoption. As organizations continue to embrace cloud technologies and the demand for secure, cloud-native solutions increases, the dominance of the cloud deployment segment is expected to persist. It provides the agility and scalability necessary to safeguard digital assets in a dynamic and interconnected environment, highlighting its crucial role in the growth and development of the Global Enterprise Firewall Hardware Market.

Regional Insights

In 2023, North America emerged as the dominant region, capturing the largest market share in the enterprise firewall hardware market. This dominance can be attributed to several key factors. The region is home to numerous large corporations, technology giants, financial institutions, and government agencies, all of which require robust cybersecurity measures to protect their operations and sensitive data. This significant demand has fostered a thriving market ecosystem for enterprise firewall solutions. North America maintains a high level of awareness and compliance with stringent data protection regulations and cybersecurity standards, prompting organizations to invest significantly in advanced firewall technologies. The region has witnessed a rise in cyber threats, such as ransomware attacks and data breaches, driving increased adoption of enterprise firewall solutions. North America boasts a well-established IT infrastructure and a tech-savvy population, which encourages early adoption of cutting-edge cybersecurity technologies, including next-generation firewalls. Furthermore, the presence of numerous cybersecurity solution providers and leading firewall manufacturers in North America has stimulated innovation and competition, offering a wide array of options for enterprises seeking effective firewall solutions.

Key Market Players

Palo Alto Networks, Inc.

Cisco Systems, Inc.

Fortinet, Inc.

Check Point Software Technologies Ltd.

Juniper Networks, Inc.

SonicWall, Inc.

WatchGuard Technologies, Inc.

Sophos Ltd.

Barracuda Networks, Inc.

Forcepoint

Report Scope:

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

Enterprise Firewall Hardware Market, By Type of Deployment:

On-premises

Cloud

Enterprise Firewall Hardware Market, By Organization:

Small and Medium

Large

Enterprise Firewall Hardware Market, By End User:

Healthcare

Manufacturing

Government

Retail

Education

Others

Enterprise Firewall Hardware Market, By Region:

North America

§ United States

§ Canada

§ Mexico

Europe

§ France

§ United Kingdom

§ Italy

§ Germany

§ Spain

§ Netherlands

§ Belgium

Asia-Pacific

§ China

§ India

§ Japan

§ Australia

§ South Korea

§ Thailand

§ Malaysia

South America

§ Brazil

§ Argentina

§ Colombia

§ Chile

Middle East & Africa

§ South Africa

§ Saudi Arabia

§ UAE

§ Turkey

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Enterprise Firewall Hardware Market.

Available Customizations:

Global Enterprise Firewall Hardware 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).

Contents

1. PRODUCT OVERVIEW

- 1.1. Market Definition
- 1.2. Scope of the Market
 - 1.2.1. Markets Covered
 - 1.2.2. Years Considered for Study
 - 1.2.3. Key Market Segmentations

2. RESEARCH METHODOLOGY

- 2.1. Objective of the Study
- 2.2. Baseline Methodology
- 2.3. Formulation of the Scope
- 2.4. Assumptions and Limitations
- 2.5. Sources of Research
 - 2.5.1. Secondary Research
 - 2.5.2. Primary Research
- 2.6. Approach for the Market Study
 - 2.6.1. The Bottom-Up Approach
 - 2.6.2. The Top-Down Approach
- 2.7. Methodology Followed for Calculation of Market Size & Market Shares
- 2.8. Forecasting Methodology
 - 2.8.1. Data Triangulation & Validation

3. EXECUTIVE SUMMARY

4. IMPACT OF COVID-19 ON GLOBAL ENTERPRISE FIREWALL HARDWARE MARKET

5. VOICE OF CUSTOMER

6. GLOBAL ENTERPRISE FIREWALL HARDWARE MARKET OVERVIEW

7. GLOBAL ENTERPRISE FIREWALL HARDWARE MARKET OUTLOOK

- 7.1. Market Size & Forecast
 - 7.1.1. By Value

7.2. Market Share & Forecast

7.2.1. By Type of Deployment (On-premises, Cloud)

7.2.2. By Organization (Small and Medium, Large)

7.2.3. By End User (Healthcare, Manufacturing, Government, Retail, Education, Others)

7.2.4. By Region

7.3. By Company (2023)

7.4. Market Map

8. NORTH AMERICA ENTERPRISE FIREWALL HARDWARE MARKET OUTLOOK

8.1. Market Size & Forecast

8.1.1. By Value

8.2. Market Share & Forecast

8.2.1. By Type of Deployment

8.2.2. By Organization

8.2.3. By End User

8.2.4. By Country

8.3. North America: Country Analysis

8.3.1. United States Enterprise Firewall Hardware Market Outlook

8.3.1.1. Market Size & Forecast

8.3.1.1.1. By Value

8.3.1.2. Market Share & Forecast

8.3.1.2.1. By Type of Deployment

8.3.1.2.2. By Organization

8.3.1.2.3. By End User

8.3.2. Canada Enterprise Firewall Hardware Market Outlook

8.3.2.1. Market Size & Forecast

8.3.2.1.1. By Value

8.3.2.2. Market Share & Forecast

8.3.2.2.1. By Type of Deployment

8.3.2.2.2. By Organization

8.3.2.2.3. By End User

8.3.3. Mexico Enterprise Firewall Hardware Market Outlook

8.3.3.1. Market Size & Forecast

8.3.3.1.1. By Value

8.3.3.2. Market Share & Forecast

8.3.3.2.1. By Type of Deployment

8.3.3.2.2. By Organization

8.3.3.2.3. By End User

9. EUROPE ENTERPRISE FIREWALL HARDWARE MARKET OUTLOOK

9.1. Market Size & Forecast

9.1.1. By Value

9.2. Market Share & Forecast

9.2.1. By Type of Deployment

9.2.2. By Organization

9.2.3. By End User

9.2.4. By Country

9.3. Europe: Country Analysis

9.3.1. Germany Enterprise Firewall Hardware Market Outlook

9.3.1.1. Market Size & Forecast

9.3.1.1.1. By Value

9.3.1.2. Market Share & Forecast

9.3.1.2.1. By Type of Deployment

9.3.1.2.2. By Organization

9.3.1.2.3. By End User

9.3.2. France Enterprise Firewall Hardware Market Outlook

9.3.2.1. Market Size & Forecast

9.3.2.1.1. By Value

9.3.2.2. Market Share & Forecast

9.3.2.2.1. By Type of Deployment

9.3.2.2.2. By Organization

9.3.2.2.3. By End User

9.3.3. United Kingdom Enterprise Firewall Hardware Market Outlook

9.3.3.1. Market Size & Forecast

9.3.3.1.1. By Value

9.3.3.2. Market Share & Forecast

9.3.3.2.1. By Type of Deployment

9.3.3.2.2. By Organization

9.3.3.2.3. By End User

9.3.4. Italy Enterprise Firewall Hardware Market Outlook

9.3.4.1. Market Size & Forecast

9.3.4.1.1. By Value

9.3.4.2. Market Share & Forecast

9.3.4.2.1. By Type of Deployment

9.3.4.2.2. By Organization

- 9.3.4.2.3. By End User
- 9.3.5. Spain Enterprise Firewall Hardware Market Outlook
 - 9.3.5.1. Market Size & Forecast
 - 9.3.5.1.1. By Value
 - 9.3.5.2. Market Share & Forecast
 - 9.3.5.2.1. By Type of Deployment
 - 9.3.5.2.2. By Organization
 - 9.3.5.2.3. By End User
- 9.3.6. Netherlands Enterprise Firewall Hardware Market Outlook
 - 9.3.6.1. Market Size & Forecast
 - 9.3.6.1.1. By Value
 - 9.3.6.2. Market Share & Forecast
 - 9.3.6.2.1. By Type of Deployment
 - 9.3.6.2.2. By Organization
 - 9.3.6.2.3. By End User
- 9.3.7. Belgium Enterprise Firewall Hardware Market Outlook
 - 9.3.7.1. Market Size & Forecast
 - 9.3.7.1.1. By Value
 - 9.3.7.2. Market Share & Forecast
 - 9.3.7.2.1. By Type of Deployment
 - 9.3.7.2.2. By Organization
 - 9.3.7.2.3. By End User

10. SOUTH AMERICA ENTERPRISE FIREWALL HARDWARE MARKET OUTLOOK

- 10.1. Market Size & Forecast
 - 10.1.1. By Value
- 10.2. Market Share & Forecast
 - 10.2.1. By Type of Deployment
 - 10.2.2. By Organization
 - 10.2.3. By End User
 - 10.2.4. By Country
- 10.3. South America: Country Analysis
 - 10.3.1. Brazil Enterprise Firewall Hardware Market Outlook
 - 10.3.1.1. Market Size & Forecast
 - 10.3.1.1.1. By Value
 - 10.3.1.2. Market Share & Forecast
 - 10.3.1.2.1. By Type of Deployment
 - 10.3.1.2.2. By Organization

- 10.3.1.2.3. By End User
- 10.3.2. Colombia Enterprise Firewall Hardware Market Outlook
 - 10.3.2.1. Market Size & Forecast
 - 10.3.2.1.1. By Value
 - 10.3.2.2. Market Share & Forecast
 - 10.3.2.2.1. By Type of Deployment
 - 10.3.2.2.2. By Organization
 - 10.3.2.2.3. By End User
- 10.3.3. Argentina Enterprise Firewall Hardware Market Outlook
 - 10.3.3.1. Market Size & Forecast
 - 10.3.3.1.1. By Value
 - 10.3.3.2. Market Share & Forecast
 - 10.3.3.2.1. By Type of Deployment
 - 10.3.3.2.2. By Organization
 - 10.3.3.2.3. By End User
- 10.3.4. Chile Enterprise Firewall Hardware Market Outlook
 - 10.3.4.1. Market Size & Forecast
 - 10.3.4.1.1. By Value
 - 10.3.4.2. Market Share & Forecast
 - 10.3.4.2.1. By Type of Deployment
 - 10.3.4.2.2. By Organization
 - 10.3.4.2.3. By End User

11. MIDDLE EAST & AFRICA ENTERPRISE FIREWALL HARDWARE MARKET OUTLOOK

- 11.1. Market Size & Forecast
 - 11.1.1. By Value
- 11.2. Market Share & Forecast
 - 11.2.1. By Type of Deployment
 - 11.2.2. By Organization
 - 11.2.3. By End User
 - 11.2.4. By Country
- 11.3. Middle East & Africa: Country Analysis
 - 11.3.1. Saudi Arabia Enterprise Firewall Hardware Market Outlook
 - 11.3.1.1. Market Size & Forecast
 - 11.3.1.1.1. By Value
 - 11.3.1.2. Market Share & Forecast
 - 11.3.1.2.1. By Type of Deployment

- 11.3.1.2.2. By Organization
- 11.3.1.2.3. By End User
- 11.3.2. UAE Enterprise Firewall Hardware Market Outlook
 - 11.3.2.1. Market Size & Forecast
 - 11.3.2.1.1. By Value
 - 11.3.2.2. Market Share & Forecast
 - 11.3.2.2.1. By Type of Deployment
 - 11.3.2.2.2. By Organization
 - 11.3.2.2.3. By End User
- 11.3.3. South Africa Enterprise Firewall Hardware Market Outlook
 - 11.3.3.1. Market Size & Forecast
 - 11.3.3.1.1. By Value
 - 11.3.3.2. Market Share & Forecast
 - 11.3.3.2.1. By Type of Deployment
 - 11.3.3.2.2. By Organization
 - 11.3.3.2.3. By End User
- 11.3.4. Turkey Enterprise Firewall Hardware Market Outlook
 - 11.3.4.1. Market Size & Forecast
 - 11.3.4.1.1. By Value
 - 11.3.4.2. Market Share & Forecast
 - 11.3.4.2.1. By Type of Deployment
 - 11.3.4.2.2. By Organization
 - 11.3.4.2.3. By End User

12. ASIA PACIFIC ENTERPRISE FIREWALL HARDWARE MARKET OUTLOOK

- 12.1. Market Size & Forecast
 - 12.1.1. By Value
- 12.2. Market Share & Forecast
 - 12.2.1. By Type of Deployment
 - 12.2.2. By Organization
 - 12.2.3. By End User
 - 12.2.4. By Country
- 12.3. Asia-Pacific: Country Analysis
 - 12.3.1. China Enterprise Firewall Hardware Market Outlook
 - 12.3.1.1. Market Size & Forecast
 - 12.3.1.1.1. By Value
 - 12.3.1.2. Market Share & Forecast
 - 12.3.1.2.1. By Type of Deployment

- 12.3.1.2.2. By Organization
- 12.3.1.2.3. By End User
- 12.3.2. India Enterprise Firewall Hardware Market Outlook
 - 12.3.2.1. Market Size & Forecast
 - 12.3.2.1.1. By Value
 - 12.3.2.2. Market Share & Forecast
 - 12.3.2.2.1. By Type of Deployment
 - 12.3.2.2.2. By Organization
 - 12.3.2.2.3. By End User
- 12.3.3. Japan Enterprise Firewall Hardware Market Outlook
 - 12.3.3.1. Market Size & Forecast
 - 12.3.3.1.1. By Value
 - 12.3.3.2. Market Share & Forecast
 - 12.3.3.2.1. By Type of Deployment
 - 12.3.3.2.2. By Organization
 - 12.3.3.2.3. By End User
- 12.3.4. South Korea Enterprise Firewall Hardware Market Outlook
 - 12.3.4.1. Market Size & Forecast
 - 12.3.4.1.1. By Value
 - 12.3.4.2. Market Share & Forecast
 - 12.3.4.2.1. By Type of Deployment
 - 12.3.4.2.2. By Organization
 - 12.3.4.2.3. By End User
- 12.3.5. Australia Enterprise Firewall Hardware Market Outlook
 - 12.3.5.1. Market Size & Forecast
 - 12.3.5.1.1. By Value
 - 12.3.5.2. Market Share & Forecast
 - 12.3.5.2.1. By Type of Deployment
 - 12.3.5.2.2. By Organization
 - 12.3.5.2.3. By End User
- 12.3.6. Thailand Enterprise Firewall Hardware Market Outlook
 - 12.3.6.1. Market Size & Forecast
 - 12.3.6.1.1. By Value
 - 12.3.6.2. Market Share & Forecast
 - 12.3.6.2.1. By Type of Deployment
 - 12.3.6.2.2. By Organization
 - 12.3.6.2.3. By End User
- 12.3.7. Malaysia Enterprise Firewall Hardware Market Outlook
 - 12.3.7.1. Market Size & Forecast

- 12.3.7.1.1. By Value
- 12.3.7.2. Market Share & Forecast
 - 12.3.7.2.1. By Type of Deployment
 - 12.3.7.2.2. By Organization
 - 12.3.7.2.3. By End User

13. MARKET DYNAMICS

- 13.1. Drivers
- 13.2. Challenges

14. MARKET TRENDS AND DEVELOPMENTS

15. COMPANY PROFILES

- 15.1. Palo Alto Networks, Inc.
 - 15.1.1. Business Overview
 - 15.1.2. Key Revenue and Financials
 - 15.1.3. Recent Developments
 - 15.1.4. Key Personnel/Key Contact Person
 - 15.1.5. Key Product/Services Offered
- 15.2. Cisco Systems, Inc.
 - 15.2.1. Business Overview
 - 15.2.2. Key Revenue and Financials
 - 15.2.3. Recent Developments
 - 15.2.4. Key Personnel/Key Contact Person
 - 15.2.5. Key Product/Services Offered
- 15.3. Fortinet, Inc.
 - 15.3.1. Business Overview
 - 15.3.2. Key Revenue and Financials
 - 15.3.3. Recent Developments
 - 15.3.4. Key Personnel/Key Contact Person
 - 15.3.5. Key Product/Services Offered
- 15.4. Check Point Software Technologies Ltd.
 - 15.4.1. Business Overview
 - 15.4.2. Key Revenue and Financials
 - 15.4.3. Recent Developments
 - 15.4.4. Key Personnel/Key Contact Person
 - 15.4.5. Key Product/Services Offered

- 15.5. Juniper Networks, Inc.
 - 15.5.1. Business Overview
 - 15.5.2. Key Revenue and Financials
 - 15.5.3. Recent Developments
 - 15.5.4. Key Personnel/Key Contact Person
 - 15.5.5. Key Product/Services Offered
- 15.6. SonicWall, Inc.
 - 15.6.1. Business Overview
 - 15.6.2. Key Revenue and Financials
 - 15.6.3. Recent Developments
 - 15.6.4. Key Personnel/Key Contact Person
 - 15.6.5. Key Product/Services Offered
- 15.7. WatchGuard Technologies, Inc.
 - 15.7.1. Business Overview
 - 15.7.2. Key Revenue and Financials
 - 15.7.3. Recent Developments
 - 15.7.4. Key Personnel/Key Contact Person
 - 15.7.5. Key Product/Services Offered
- 15.8. Sophos Ltd.
 - 15.8.1. Business Overview
 - 15.8.2. Key Revenue and Financials
 - 15.8.3. Recent Developments
 - 15.8.4. Key Personnel/Key Contact Person
 - 15.8.5. Key Product/Services Offered
- 15.9. Barracuda Networks, Inc.
 - 15.9.1. Business Overview
 - 15.9.2. Key Revenue and Financials
 - 15.9.3. Recent Developments
 - 15.9.4. Key Personnel/Key Contact Person
 - 15.9.5. Key Product/Services Offered
- 15.10. Forcepoint
 - 15.10.1. Business Overview
 - 15.10.2. Key Revenue and Financials
 - 15.10.3. Recent Developments
 - 15.10.4. Key Personnel/Key Contact Person
 - 15.10.5. Key Product/Services Offered

16. STRATEGIC RECOMMENDATIONS

17. ABOUT US & DISCLAIMER

I would like to order

Product name: Enterprise Firewall Hardware Market - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Type of Deployment (On-premises, Cloud), By Organization (Small and Medium, Large), By End User (Healthcare, Manufacturing, Government, Retail, Education, Others), By Region, and By Competition, 2019-2029F

Product link: <https://marketpublishers.com/r/E0A4BE6BFF6CEN.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/E0A4BE6BFF6CEN.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**

Customer signature _____

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