

# **Web Application Firewall Market– Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution (Hardware Appliances, Virtual Appliances, Cloud-Based), Services (Consulting, Support and Maintenance, Training and Education, Professional Services, System Integration)), By Organization Size (Small and Medium-Sized Enterprises, Large Enterprises), By Industry Vertical (BFSI, Retail, IT and Telecommunications, Government and Defence, Healthcare, Energy and Utilities, Education, Others), By Region, By Competition , 2018-2028**

<https://marketpublishers.com/r/WC3B61AFDAF0EN.html>

Date: October 2023

Pages: 178

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

ID: WC3B61AFDAF0EN

## **Abstracts**

Global Web Application Firewall Market has valued at USD 6.1 Billion in 2022 and is anticipated to project robust growth in the forecast period with a CAGR of 17.5% through 2028. The Global Web Application Firewall (WAF) Market has witnessed substantial growth in recent years, driven by the escalating cyber threat landscape and the ever-increasing reliance on web applications. WAFs serve as critical defense mechanisms, safeguarding organizations from a plethora of online vulnerabilities, including data breaches, application layer attacks, and distributed denial of service (DDoS) attacks.

Several factors contribute to the rising prominence of WAF solutions. Firstly, the surge in e-commerce, cloud adoption, and remote work has expanded the attack surface,

making web applications vulnerable targets. Secondly, stringent regulatory requirements, such as GDPR and CCPA, have compelled businesses to bolster their cybersecurity posture, further fueling the demand for WAFs. Moreover, the evolution of sophisticated attack techniques necessitates advanced and adaptive security measures, which WAFs offer through real-time monitoring, threat detection, and automatic mitigation.

Key players in the market are continually innovating, introducing AI and machine learning capabilities to enhance threat detection and response. As organizations prioritize web security, the Global WAF Market is expected to continue its growth trajectory, offering robust protection in an increasingly interconnected digital landscape.

## Key Market Drivers

### Rise in Cybersecurity Threats and Attacks

The increasing frequency and sophistication of cyber threats and attacks have become a major concern for organizations worldwide. Web applications are often targeted by hackers to gain unauthorized access, steal sensitive data, or disrupt business operations. As a result, there is a growing demand for robust security solutions like web application firewalls (WAFs) that can protect against common web-based attacks, such as SQL injection, cross-site scripting (XSS), and distributed denial-of-service (DDoS) attacks. The rise in cybersecurity threats has prompted organizations to invest in WAF solutions to safeguard their web applications and ensure the integrity and confidentiality of their data.

### Stringent Regulatory Compliance Requirements

Various industries, including finance, healthcare, and e-commerce, are subject to stringent regulatory compliance requirements regarding data protection and privacy. Compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR) mandate organizations to implement adequate security measures to protect sensitive customer information. Web application firewalls play a crucial role in meeting these compliance requirements by providing protection against unauthorized access, data breaches, and other security vulnerabilities. The need to adhere to regulatory standards has driven the adoption of WAF solutions across industries.

## Increasing Adoption of Cloud-based Applications

The rapid adoption of cloud computing and the migration of applications to the cloud have transformed the business landscape. Cloud-based applications offer scalability, flexibility, and cost-efficiency, but they also introduce new security challenges. Organizations need to secure their cloud-based applications from potential threats and vulnerabilities. Web application firewalls provide an additional layer of security by monitoring and filtering incoming and outgoing traffic to cloud-based applications, ensuring that only legitimate requests are processed. The increasing adoption of cloud-based applications has fueled the demand for WAF solutions to protect critical business data and maintain the availability and performance of cloud-based services.

## Growing Awareness of Web Application Security

As organizations become more aware of the potential risks associated with web application vulnerabilities, there is a growing emphasis on web application security. High-profile data breaches and cyber attacks have highlighted the need for proactive measures to protect web applications from exploitation. Web application firewalls are recognized as an essential component of a comprehensive security strategy, as they can detect and mitigate threats in real-time, preventing unauthorized access and data breaches. The growing awareness of web application security risks has led to increased investments in WAF solutions to fortify the security posture of organizations.

## Integration of Artificial Intelligence and Machine Learning Technologies

The integration of artificial intelligence (AI) and machine learning (ML) technologies into web application firewalls has revolutionized the way security threats are detected and mitigated. AI and ML algorithms can analyze vast amounts of data, identify patterns, and detect anomalies in real-time, enabling WAF solutions to adapt and respond to evolving threats effectively. These advanced technologies enhance the accuracy and efficiency of web application firewalls, reducing false positives and false negatives. The integration of AI and ML technologies has significantly improved the threat detection capabilities of WAF solutions, making them more intelligent and effective in safeguarding web applications.

## Key Market Challenges

### Lack of Awareness and Understanding

A significant challenge in the global web application firewall (WAF) market is the lack of awareness and understanding among organizations regarding the importance and benefits of implementing WAF solutions. This lack of awareness often stems from businesses, particularly small and medium-sized enterprises (SMEs), not fully comprehending the potential risks and vulnerabilities associated with web applications. As a result, organizations may be hesitant to invest in WAF solutions, leaving their web applications susceptible to attacks. To address this challenge, it is crucial to educate organizations about the significance of web application security and the role that WAFs play in mitigating risks and protecting against cyber threats.

Educational initiatives should focus on raising awareness about the potential consequences of web application vulnerabilities, such as data breaches, unauthorized access, and service disruptions. Organizations need to understand that web applications are prime targets for hackers and that a single security breach can have severe financial, reputational, and legal implications. By highlighting real-world examples and case studies, organizations can grasp the tangible impact of inadequate web application security.

Furthermore, organizations should be educated about the specific benefits of implementing WAF solutions. This includes emphasizing how WAFs can detect and block common web-based attacks, such as SQL injection and cross-site scripting (XSS), as well as providing protection against emerging threats. Organizations should also be made aware of the additional layers of security that WAFs offer, such as traffic filtering, access control, and threat intelligence integration.

### Complexity and Integration Issues

The implementation and management of web application firewall (WAF) solutions can be a complex task, particularly for organizations that have limited IT resources or expertise. The process of configuring and fine-tuning WAFs to effectively protect web applications requires technical knowledge and ongoing monitoring. Additionally, integrating WAF solutions with existing IT infrastructure and applications can present challenges, as compatibility issues may arise. These difficulties can result in delays in implementation or suboptimal performance of the WAF solutions. To overcome these challenges, it is crucial to simplify the deployment and management processes associated with WAFs. This can be achieved by providing user-friendly interfaces and intuitive configuration options that make it easier for organizations to set up and customize their WAF solutions. Comprehensive support and guidance should also be offered to assist organizations in navigating the complexities of integrating WAFs into

their existing security infrastructure. This support can include documentation, tutorials, and access to technical experts who can provide assistance and address any issues that may arise during the implementation process. By simplifying the deployment and management of WAF solutions and offering robust support, organizations can overcome the complexities associated with integrating WAFs into their security infrastructure. This will help ensure a smooth and efficient implementation process, leading to optimal performance and enhanced protection for web applications.

### False Positives and Performance Impact

Web application firewalls (WAFs) play a vital role in identifying and mitigating potential threats, but there is a challenge of false positives, where legitimate traffic is mistakenly flagged as malicious. These false positives can have detrimental effects on normal business operations and lead to frustration among users. Moreover, the performance of web applications can be impacted by the introduction of WAFs, particularly when dealing with high volumes of traffic. Striking the right balance between security and performance is crucial to ensure that WAF solutions effectively protect web applications without causing unnecessary disruptions. To address this challenge, continuous improvement in WAF algorithms and technologies is necessary. By refining these algorithms, WAFs can minimize the occurrence of false positives, accurately distinguishing between legitimate and malicious traffic. Additionally, optimizing the performance of WAF solutions is essential to minimize latency and ensure smooth operation of web applications, even under heavy traffic loads. This ongoing enhancement of WAF capabilities will enable organizations to maintain a secure web environment while delivering a seamless user experience.

### Key Market Trends

#### Rise in Sophisticated Cyber Attacks

The global market for web application firewalls (WAFs) is experiencing an increase in the number of sophisticated cyber attacks specifically targeting web applications. Hackers are continuously evolving their techniques to exploit vulnerabilities and gain unauthorized access to sensitive data. Consequently, there is a rising demand for advanced WAF solutions that can effectively detect and mitigate these sophisticated attacks. In response to this demand, WAF vendors are concentrating their efforts on developing intelligent and adaptive solutions that possess the capability to analyze traffic patterns, identify anomalies, and offer real-time protection against emerging threats. These advanced WAF solutions leverage technologies such as artificial

intelligence and machine learning to enhance their threat detection capabilities. By analyzing vast amounts of data, these solutions can identify patterns and detect anomalies in real-time, enabling organizations to respond swiftly to evolving threats. The goal is to provide organizations with proactive defense mechanisms that can adapt to the ever-changing threat landscape. With the continuous advancements in WAF technologies, organizations can benefit from robust security measures that effectively safeguard their web applications and protect sensitive data from unauthorized access. By investing in intelligent and adaptive WAF solutions, organizations can stay one step ahead of cyber attackers and ensure the integrity and confidentiality of their web applications.

### Shift towards Cloud-based WAF Solutions

The global market is experiencing a significant shift towards cloud-based web application firewall (WAF) solutions. This shift is driven by the increasing adoption of cloud computing and the migration of applications to the cloud. Organizations are now seeking WAF solutions that can seamlessly integrate with their cloud infrastructure to ensure comprehensive security for their web applications.

Cloud-based WAF solutions offer several advantages. Firstly, they provide scalability, allowing organizations to easily adjust their resources based on the changing demands of their web applications. This scalability ensures that the WAF solution can handle varying levels of traffic and effectively protect the applications during peak usage periods.

Cloud-based WAF solutions offer flexibility. They can be easily deployed and managed across multiple cloud environments, providing organizations with the freedom to choose the cloud platform that best suits their needs. This flexibility enables seamless integration with existing cloud infrastructure and ensures that the WAF solution can adapt to the specific requirements of the organization.

### Integration of Artificial Intelligence and Machine Learning

The integration of artificial intelligence (AI) and machine learning (ML) technologies into WAF solutions is a significant trend in the market. AI and ML algorithms can analyze vast amounts of data, identify patterns, and detect anomalies in real-time, enabling WAF solutions to adapt and respond to evolving threats effectively. These advanced technologies enhance the accuracy and efficiency of WAF solutions, reducing false positives and false negatives. WAF vendors are investing in AI and ML capabilities to



enhance threat detection, automate security operations, and provide proactive defense against emerging threats.

## Segmental Insights

### Component Insights

In 2022, the cloud-based segment dominated the global web application firewall (WAF) market and is expected to maintain its dominance during the forecast period. Cloud-based WAF solutions have gained significant traction due to their numerous advantages and the increasing adoption of cloud computing. These solutions offer scalability, flexibility, and cost-efficiency, making them highly attractive to organizations seeking effective web application security.

Cloud-based WAF solutions provide organizations with the ability to protect their web applications without the need for extensive on-premises infrastructure. This eliminates the costs associated with hardware appliances and the maintenance and upgrades required for physical devices. Instead, organizations can leverage the infrastructure provided by cloud service providers, paying for the resources they use on a subscription basis. This cost-effective approach allows organizations to allocate their resources more efficiently and invest in other critical areas of their business.

Furthermore, cloud-based WAF solutions offer scalability, allowing organizations to easily adjust their resources based on the changing demands of their web applications. This scalability ensures that the WAF solution can handle varying levels of traffic and effectively protect the applications during peak usage periods. Additionally, cloud-based solutions provide flexibility, as they can be easily deployed and managed across multiple cloud environments. This flexibility enables seamless integration with existing cloud infrastructure and ensures that the WAF solution can adapt to the specific requirements of the organization.

Moreover, cloud-based WAF solutions provide centralized management and monitoring capabilities. Organizations can configure and manage their WAF policies from a single, centralized dashboard, regardless of the number of web applications or cloud environments they have. This centralized approach simplifies the management process, enhances visibility, and enables organizations to monitor and respond to security incidents in real-time.

## Organization Size Insights

In 2022, the large enterprises segment dominated the global web application firewall (WAF) market and is expected to maintain its dominance during the forecast period. Large enterprises have been at the forefront of adopting advanced cybersecurity solutions, including WAFs, to protect their web applications from evolving threats.

Large enterprises typically have larger budgets and resources compared to small and medium-sized enterprises (SMEs), allowing them to invest in robust security measures. They often handle a higher volume of web traffic and have a greater number of web applications to protect, making the implementation of WAF solutions a critical priority. These organizations understand the potential risks and vulnerabilities associated with web applications and are proactive in implementing WAFs to safeguard their digital assets.

Moreover, large enterprises often operate in industries that handle sensitive customer data, such as finance, healthcare, and e-commerce. The protection of this data is of utmost importance to maintain customer trust and comply with regulatory requirements. WAF solutions provide an essential layer of defense against cyber threats targeting web applications, ensuring the confidentiality, integrity, and availability of sensitive information.

Additionally, large enterprises have dedicated IT teams and resources to manage and monitor WAF solutions effectively. They can allocate personnel and expertise to configure and fine-tune WAFs, ensuring optimal performance and threat detection. This level of commitment and investment in web application security gives large enterprises a competitive advantage in mitigating risks and maintaining a strong security posture.

## Regional Insights

In 2022, North America dominated the global web application firewall (WAF) market and is expected to maintain its dominance during the forecast period. North America has been at the forefront of technological advancements and has a strong presence of major players in the cybersecurity industry. The region's dominance can be attributed to several factors. Firstly, North America has a high concentration of large enterprises that prioritize robust web application security. These organizations have significant budgets and resources to invest in advanced cybersecurity solutions, including WAFs, to protect their web applications from evolving threats. The presence of major industries such as finance, healthcare, and e-commerce further drives the demand for WAF solutions in the region.



Secondly, North America has witnessed a significant increase in cyber attacks targeting web applications. The region has experienced high-profile data breaches and cyber incidents, which have raised awareness about the importance of web application security. This heightened awareness has led to increased adoption of WAF solutions among organizations in North America.

Furthermore, North America has a mature and well-established cybersecurity ecosystem. The region is home to leading cybersecurity vendors, service providers, and research institutions that contribute to the development and innovation of WAF technologies. This ecosystem fosters collaboration and knowledge sharing, enabling organizations in North America to stay ahead of emerging threats and implement effective WAF strategies.

### Key Market Players

Imperva Inc.

Akamai Technologies, Inc.

Barracuda Networks, Inc.

F5 Networks, Inc.

Fortinet, Inc.

Citrix Systems, Inc.

Radware Ltd.

Cloudflare, Inc.

Trustwave Holdings, Inc.

NSFOCUS Information Technology Co., Ltd.

Penta Security Systems Inc.

Positive Technologies

## Report Scope:

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

### Web Application Firewall Market, By Component:

Solution

Services

### Web Application Firewall Market, By Organization Size:

Small and Medium-Sized Enterprises

Large Enterprises

### Web Application Firewall Market, By Industry Vertical:

BFSI

Retail

IT and Telecommunications

Government and Defence

Healthcare

Energy and Utilities

Education

Others

### Web Application Firewall Market, By Region:

## North America

United States

Canada

Mexico

## Europe

France

United Kingdom

Italy

Germany

Spain

Belgium

## Asia-Pacific

China

India

Japan

Australia

South Korea

Indonesia

Vietnam

## South America

Brazil

Argentina

Colombia

Chile

Peru

Middle East & Africa

South Africa

Saudi Arabia

UAE

Turkey

Israel

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Web Application Firewall Market.

Available Customizations:

Global Web Application Firewall 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 WEB APPLICATION FIREWALL MARKET**

### **5. VOICE OF CUSTOMER**

### **6. GLOBAL WEB APPLICATION FIREWALL MARKET OVERVIEW**

### **7. GLOBAL WEB APPLICATION FIREWALL MARKET OUTLOOK**

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

7.2.1. By Component (Solution (Hardware Appliances, Virtual Appliances, Cloud-Based), Services (Consulting, Support and Maintenance, Training and Education, Professional Services, System Integration))

7.2.2. By Organization Size (Small and Medium-Sized Enterprises, Large Enterprises)

7.2.3. By Industry Vertical (BFSI, Retail, IT and Telecommunications, Government and Defence, Healthcare, Energy and Utilities, Education, Others)

7.2.4. By Region (North America, Europe, South America, Middle East & Africa, Asia Pacific)

7.3. By Company (2022)

7.4. Market Map

## **8. NORTH AMERICA WEB APPLICATION FIREWALL MARKET OUTLOOK**

8.1. Market Size & Forecast

8.1.1. By Value

8.2. Market Share & Forecast

8.2.1. By Component

8.2.2. By Organization Size

8.2.3. By Industry Vertical

8.2.4. By Country

8.3. North America: Country Analysis

8.3.1. United States Web Application Firewall 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 Component

8.3.1.2.2. By Organization Size

8.3.1.2.3. By Industry Vertical

8.3.2. Canada Web Application Firewall 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 Component

8.3.2.2.2. By Organization Size

8.3.2.2.3. By Industry Vertical

8.3.3. Mexico Web Application Firewall 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 Component
- 8.3.3.2.2. By Organization Size
- 8.3.3.2.3. By Industry Vertical

## **9. EUROPE WEB APPLICATION FIREWALL MARKET OUTLOOK**

### 9.1. Market Size & Forecast

#### 9.1.1. By Value

### 9.2. Market Share & Forecast

#### 9.2.1. By Component

#### 9.2.2. By Organization Size

#### 9.2.3. By Industry Vertical

#### 9.2.4. By Country

### 9.3. Europe: Country Analysis

#### 9.3.1. Germany Web Application Firewall 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 Component

###### 9.3.1.2.2. By Organization Size

###### 9.3.1.2.3. By Industry Vertical

#### 9.3.2. France Web Application Firewall 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 Component

###### 9.3.2.2.2. By Organization Size

###### 9.3.2.2.3. By Industry Vertical

#### 9.3.3. United Kingdom Web Application Firewall 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 Component

###### 9.3.3.2.2. By Organization Size

###### 9.3.3.2.3. By Industry Vertical

#### 9.3.4. Italy Web Application Firewall 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 Component
- 9.3.4.2.2. By Organization Size
- 9.3.4.2.3. By Industry Vertical
- 9.3.5. Spain Web Application Firewall 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 Component
    - 9.3.5.2.2. By Organization Size
    - 9.3.5.2.3. By Industry Vertical
- 9.3.6. Belgium Web Application Firewall 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 Component
    - 9.3.6.2.2. By Organization Size
    - 9.3.6.2.3. By Industry Vertical

## **10. SOUTH AMERICA WEB APPLICATION FIREWALL MARKET OUTLOOK**

- 10.1. Market Size & Forecast
  - 10.1.1. By Value
- 10.2. Market Share & Forecast
  - 10.2.1. By Component
  - 10.2.2. By Organization Size
  - 10.2.3. By Industry Vertical
  - 10.2.4. By Country
- 10.3. South America: Country Analysis
  - 10.3.1. Brazil Web Application Firewall 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 Component
      - 10.3.1.2.2. By Organization Size
      - 10.3.1.2.3. By Industry Vertical
  - 10.3.2. Colombia Web Application Firewall 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 Component
- 10.3.2.2.2. By Organization Size
- 10.3.2.2.3. By Industry Vertical
- 10.3.3. Argentina Web Application Firewall 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 Component
    - 10.3.3.2.2. By Organization Size
    - 10.3.3.2.3. By Industry Vertical
- 10.3.4. Chile Web Application Firewall 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 Component
    - 10.3.4.2.2. By Organization Size
    - 10.3.4.2.3. By Industry Vertical
- 10.3.5. Peru Web Application Firewall Market Outlook
  - 10.3.5.1. Market Size & Forecast
    - 10.3.5.1.1. By Value
  - 10.3.5.2. Market Share & Forecast
    - 10.3.5.2.1. By Component
    - 10.3.5.2.2. By Organization Size
    - 10.3.5.2.3. By Industry Vertical

## **11. MIDDLE EAST & AFRICA WEB APPLICATION FIREWALL MARKET OUTLOOK**

- 11.1. Market Size & Forecast
  - 11.1.1. By Value
- 11.2. Market Share & Forecast
  - 11.2.1. By Component
  - 11.2.2. By Organization Size
  - 11.2.3. By Industry Vertical
  - 11.2.4. By Country
- 11.3. Middle East & Africa: Country Analysis
  - 11.3.1. Saudi Arabia Web Application Firewall 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 Component
- 11.3.1.2.2. By Organization Size
- 11.3.1.2.3. By Industry Vertical
- 11.3.2. UAE Web Application Firewall 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 Component
    - 11.3.2.2.2. By Organization Size
    - 11.3.2.2.3. By Industry Vertical
- 11.3.3. South Africa Web Application Firewall 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 Component
    - 11.3.3.2.2. By Organization Size
    - 11.3.3.2.3. By Industry Vertical
- 11.3.4. Turkey Web Application Firewall 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 Component
    - 11.3.4.2.2. By Organization Size
    - 11.3.4.2.3. By Industry Vertical
- 11.3.5. Israel Web Application Firewall Market Outlook
  - 11.3.5.1. Market Size & Forecast
    - 11.3.5.1.1. By Value
  - 11.3.5.2. Market Share & Forecast
    - 11.3.5.2.1. By Component
    - 11.3.5.2.2. By Organization Size
    - 11.3.5.2.3. By Industry Vertical

## **12. ASIA PACIFIC WEB APPLICATION FIREWALL MARKET OUTLOOK**

- 12.1. Market Size & Forecast
  - 12.1.1. By Component
  - 12.1.2. By Organization Size
  - 12.1.3. By Industry Vertical
  - 12.1.4. By Country

- 12.2. Asia-Pacific: Country Analysis
  - 12.2.1. China Web Application Firewall Market Outlook
    - 12.2.1.1. Market Size & Forecast
      - 12.2.1.1.1. By Value
    - 12.2.1.2. Market Share & Forecast
      - 12.2.1.2.1. By Component
      - 12.2.1.2.2. By Organization Size
      - 12.2.1.2.3. By Industry Vertical
  - 12.2.2. India Web Application Firewall Market Outlook
    - 12.2.2.1. Market Size & Forecast
      - 12.2.2.1.1. By Value
    - 12.2.2.2. Market Share & Forecast
      - 12.2.2.2.1. By Component
      - 12.2.2.2.2. By Organization Size
      - 12.2.2.2.3. By Industry Vertical
  - 12.2.3. Japan Web Application Firewall Market Outlook
    - 12.2.3.1. Market Size & Forecast
      - 12.2.3.1.1. By Value
    - 12.2.3.2. Market Share & Forecast
      - 12.2.3.2.1. By Component
      - 12.2.3.2.2. By Organization Size
      - 12.2.3.2.3. By Industry Vertical
  - 12.2.4. South Korea Web Application Firewall Market Outlook
    - 12.2.4.1. Market Size & Forecast
      - 12.2.4.1.1. By Value
    - 12.2.4.2. Market Share & Forecast
      - 12.2.4.2.1. By Component
      - 12.2.4.2.2. By Organization Size
      - 12.2.4.2.3. By Industry Vertical
  - 12.2.5. Australia Web Application Firewall Market Outlook
    - 12.2.5.1. Market Size & Forecast
      - 12.2.5.1.1. By Value
    - 12.2.5.2. Market Share & Forecast
      - 12.2.5.2.1. By Component
      - 12.2.5.2.2. By Organization Size
      - 12.2.5.2.3. By Industry Vertical
  - 12.2.6. Indonesia Web Application Firewall Market Outlook
    - 12.2.6.1. Market Size & Forecast
      - 12.2.6.1.1. By Value

- 12.2.6.2. Market Share & Forecast
  - 12.2.6.2.1. By Component
  - 12.2.6.2.2. By Organization Size
  - 12.2.6.2.3. By Industry Vertical
- 12.2.7. Vietnam Web Application Firewall Market Outlook
  - 12.2.7.1. Market Size & Forecast
    - 12.2.7.1.1. By Value
  - 12.2.7.2. Market Share & Forecast
    - 12.2.7.2.1. By Component
    - 12.2.7.2.2. By Organization Size
    - 12.2.7.2.3. By Industry Vertical

## **13. MARKET DYNAMICS**

- 13.1. Drivers
- 13.2. Challenges

## **14. MARKET TRENDS AND DEVELOPMENTS**

## **15. COMPANY PROFILES**

- 15.1. Imperva 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. Akamai Technologies, 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. Barracuda Networks, 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. F5 Networks, Inc.
  - 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. Fortinet, 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. Citrix Systems, 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. Radware Ltd.
  - 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. Cloudflare, Inc.
  - 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. Trustwave Holdings, 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. NSFOCUS Information Technology Co., Ltd.
  - 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

#### 15.11. Penta Security Systems Inc.

- 15.11.1. Business Overview
- 15.11.2. Key Revenue and Financials
- 15.11.3. Recent Developments
- 15.11.4. Key Personnel/Key Contact Person
- 15.11.5. Key Product/Services Offered

#### 15.12. Positive Technologies

- 15.12.1. Business Overview
- 15.12.2. Key Revenue and Financials
- 15.12.3. Recent Developments
- 15.12.4. Key Personnel/Key Contact Person
- 15.12.5. Key Product/Services Offered

## **16. STRATEGIC RECOMMENDATIONS**

## **17. ABOUT US & DISCLAIMER**

## I would like to order

Product name: Web Application Firewall Market– Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solution (Hardware Appliances, Virtual Appliances, Cloud-Based), Services (Consulting, Support and Maintenance, Training and Education, Professional Services, System Integration)), By Organization Size (Small and Medium-Sized Enterprises, Large Enterprises), By Industry Vertical (BFSI, Retail, IT and Telecommunications, Government and Defence, Healthcare, Energy and Utilities, Education, Others), By Region, By Competition , 2018-2028

Product link: <https://marketpublishers.com/r/WC3B61AFDAF0EN.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](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/WC3B61AFDAF0EN.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