Web Application Firewall (WAF) Global Market Analysis
New Technologies and Threats Collide to Create Expanded Opportunities

A Research Report Excerpt

Prepared By:
Chris Rodriguez
Senior Industry Analyst, Information & Network Security
Market Overview

• Web Applications and the Threat Landscape
  o Web applications are valuable tools for businesses of all sizes. These applications enable businesses to communicate with customers, potential customers, employees, partners, and other information technology (IT) systems.
  o By definition, Web applications must be open, interactive, and accessible from all parts of the world and at all times of the day.
  o Network security technologies such as NGFWs or intrusion prevention systems (IPS) have very limited insight or control over Web traffic. As a result, Web applications are particularly vulnerable components in an IT infrastructure.
  o Most organizations have taken basic steps to protect their Web applications, including deploying WAF and testing and patching application vulnerabilities.
  o WAF operates at the application layer and can analyze full sessions and application layer protocols that an IPS cannot see.
    ▪ WAF solutions deployed as full reverse proxies can alter the contents of application layer traffic and sessions to filter attack traffic or insert security controls.
    ▪ WAF also provides a means to deploy a virtual patch to protect an application until it can be patched.

Source: Frost & Sullivan
Market Overview (continued)

• Web Application Firewall Trajectory
  o Early WAF solutions focused on preventing exploitation of application vulnerabilities and defending against the Open Web Application Security Project (OWASP) Top 10 threats such as cross-site scripting and SQL injection.
  o Yet, Web threats have evolved tremendously over the years. Hackers have moved from simple attacks to more sophisticated or efficient automated attacks that challenge legacy security tools.
  o Furthermore, WAF solutions were difficult to deploy for many customers.
    ▪ WAF solutions require time and technical expertise to deploy and maintain.
    ▪ Web applications change frequently and present a “moving target” for the WAF.
    ▪ Early WAF solutions were prone to high rates of distracting false positives.
  o As a result, WAF vendors made significant investments in research and development of new detection technologies and integration with dynamic application security testing tools.
  o WAF vendors have addressed many of these challenges in recent years.

Source: Frost & Sullivan
Market Overview (continued)

• Market Outlook
  o Advanced threat actors are leveraging automated attacks and logic-based exploits, which require modern WAF solutions to properly address.
  o The risk of catastrophic security breach increases dramatically without a WAF deployment. Many customers now understand the need for a WAF.
  o Certain industry regulations specifically require businesses to deploy WAF.
  o Additionally, new Web technologies such as HTTP 2.0, Extensible Markup Language (XML), and JavaScript Object Notation (JSON) require modern WAF technologies.
  o Consequently, demand for WAF is growing.

• Challenges
  o While demand for WAF grows, the WAF market continues to evolve.
  o Businesses increasingly expect WAF to be an integrated component of ADCs, CDN services, distributed denial of service (DDoS) attack mitigation services, and NGFWs.
  o While stand-alone WAFs will provide the leading security technologies, integrated WAF can meet the needs of many organizations.
  o There is also an expansion in the tool sets required to secure Web applications such as bot detection and management capabilities.

Source: Frost & Sullivan
Market Overview (continued)

- The State of the WAF Market
  - Currently, the WAF market is represented primarily by few pure-play application security companies, and networking companies with added WAF functionality.
  - For example, F5 and Citrix offer modules for WAF and related application security technologies as extensions for their ADC and load balancing products.
  - Akamai and CloudFlare are two well known CDN service providers that offer Web security in addition to their application delivery and performance solutions.
## Drivers

### WAF Market: Key Market Drivers, Global, 2016–2020

<table>
<thead>
<tr>
<th>Market Drivers</th>
<th>1–2 years</th>
<th>3–4 years</th>
<th>5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAF solutions are necessary for compliance with industry and government regulations</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Customers understand the need to protect Web applications</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Vendors have addressed customer concerns about usability and effectiveness</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Convergence of security and performance solutions enhances customer value</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Encryption and new Web technologies require modern WAF protections</td>
<td>H</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Web applications are increasingly important to businesses</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Note: Drivers & Restraints are ranked in order of impact. Source: Frost & Sullivan
Drivers Explained

- **WAF solutions are necessary for compliance with industry and government regulations**
  - Certain industry and government regulations require deployment of a WAF solution, either explicitly or implicitly. For example, the Payment Card Industry Data Security Standard (PCI-DSS) is a well-known and important regulation that drives WAF adoption.
    - Section 6.6 specifically outlines WAF as one of two options for securing Web applications. According to the PCI Security Standards Council, “WAF functionality can be implemented in software or hardware, running in an appliance device, or in a typical server running a common operating system. It may be a stand-alone device or integrated into other network components.”*
  - The other option, application security testing, may not be a feasible option for businesses that do not own the source code or in cases where a large number of applications or updates make regular testing and patching cost prohibitive.
  - Companies that fail to meet PCI-DSS requirements may be subject to penalties that include fines and suspended privileges.
  - Other regulations contributing towards WAF adoption include the:
    - Gramm-Leach-Bliley (GLB) Act
    - Health Information Technology for Economic and Clinical Health (HITECH) Act
    - Health Insurance Portability and Accountability Act (HIPAA)
    - National Institute of Standards and Technology (NIST 800–53, Rev.4)

Drivers Explained (continued)

- **Customers understand the need to protect Web applications**
  - Businesses are negatively impacted by data breaches in a number of ways:
    - Lost end-user trust resulting in reduced Web traffic.
    - End users become wary of shopping online or sharing personal information with online businesses.
    - Lawsuits, settlements, penalties, and fines in the millions of dollars.
  - Additionally, WAF customers are generally aware of the need for a dedicated WAF solution to address application layer-based threats.
  - WAF is now considered an essential security tool along with NGFW, IPS, endpoint security, vulnerability management, security information and event management (SIEM), and encryption.*

*Data about the information and network security markets is provided in the Enterprise Security Tracker 2016, Frost & Sullivan, February 2016, available [here](#). Source: Frost & Sullivan
Drivers Explained (continued)

• **Vendors have addressed customer concerns about usability and effectiveness**
  
  o WAF has a track record of difficult and failed deployments for multiple reasons as discussed in the restraints section [here](#).
  
  o In order to lower barriers to adoption, WAF vendors have focused on minimizing the pain points traditionally associated with WAF such as deployment difficulty and security ineffectiveness.
  
  o Features such as dynamic application profiling enable rapid and simplified deployment.
    
    • Cloud-based services can be deployed in minutes and are offered as fully managed security services.
  
  o In recent years, WAF vendors have invested heavily in improving the threat detection capabilities of their products including threat detection algorithms, threat research, and device reputation capabilities.
    
    • As a result, false positive rates are minimal across all products. WAFs can now be deployed reliably in full blocking mode.

Source: Frost & Sullivan
Drivers Explained (continued)

• Convergence of security and performance solutions enhances customer value
  o Applications that are unavailable, slow, or untrustworthy approaches uselessness to end users and can drive customers to competing Web sites. Businesses require solutions to all of these challenges equally.
  o Essentially, application security and performance tools have similar end goals—to ensure availability of a Web site and applications for end users by meeting minimum expectations for speed, functionality, and trustworthiness.
  o As a result, WAF is often offered as an add-on module for ADCs, load balancers, or NGFWs.
    • Many CDN service providers offer WAF as an additional, optional service.
    • WAF and DDoS mitigation solutions provide a degree of overlapping functionality for protecting Web applications. However, neither is effective as a total replacement for the other.*
  o The convergence of WAF and application delivery and performance applications will enhance customer value and help customers to justify their investments.

*For more data and analysis of the DDoS mitigation market please read DDoS Mitigation Global Market Analysis, Frost & Sullivan, November 2015, available here. Source: Frost & Sullivan
Drivers Explained (continued)

- Encryption and new Web technologies require modern WAF protections
  - XML and JSON are examples of new Web technologies that present challenges for legacy WAFs.
    - These technologies require WAFs that can validate these transactions and detect specific attacks against these technologies.
  - HTTPS, the encrypted version of HTTP, is increasing in prevalence. Up to 24% of Web traffic is now represented by HTTPS, according to the HTTP Archive.
  - The increase in encrypted Web traffic will challenge cloud WAFs and appliances in different ways.
    - Cloud WAF providers will require customers to share their private Secure Sockets Layer (SSL) keys with them, which some customers may be wary to do.
    - Appliances can perform SSL inspection but will require specialized hardware to keep up with the processing demands needed to decrypt, inspect, and then re-encrypt traffic.
  - Additionally, HTTP/2 will not explicitly require encryption of all traffic but to date, browsers do not support unencrypted HTTP/2 traffic.
• Web applications are increasingly important to businesses
  o Web properties are essential lines of communications with customers, partners, and investors.
  o Web sites allow businesses to reach a global marketplace easily and Web applications provide the functionality to interact with end users.
    • A registration form and login are examples of Web applications that are common across all types of industries around the world.
    • Some businesses utilize vertical-specific applications such as a shopping cart application in the retail industry or a mortgage calculator in the financial industry.
  o Web applications are growing in complexity as tracked by The HTTP Archive.

Source: Frost & Sullivan
## Competitive Environment

### Total WAF Market: Competitive Structure

**Global, 2015**

<table>
<thead>
<tr>
<th>Number of Companies in the Market</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Competitive Factors</strong></td>
<td>Accuracy, advanced features, integration, usability, scalability, cost of ownership</td>
</tr>
<tr>
<td><strong>Key End-user Groups</strong></td>
<td>Information security, development, operations teams</td>
</tr>
<tr>
<td><strong>Major Market Participants</strong></td>
<td>Akamai, F5 Networks, Imperva</td>
</tr>
<tr>
<td><strong>Market Share of Top 3 Competitors</strong></td>
<td>56.0%</td>
</tr>
<tr>
<td><strong>Other Notable Market Participants</strong></td>
<td>Barracuda Networks, Citrix, CloudFlare, Fortinet, NSFOCUS, Penta Security, Radware</td>
</tr>
<tr>
<td><strong>Distribution Structure</strong></td>
<td>VARs and systems integrators, distributors, direct</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan
Competitive Environment Discussion

- The WAF market is dominated by a handful of vendors.
  - Akamai, F5 Networks, and Imperva maintain the majority of market revenue and are typically on customer “short lists.”
- WAF is an important strategic component for companies that develop and sell ADCs, load balancers, NGFWs, and CDN services.
  - There are few pure-play WAF vendors.
- The Frost & Sullivan report titled “Network Security Platform Managed Security Service Provider (MSSP) Vendor Rankings for North America” provides insight into the WAFs that are most deployed by MSSPs to offer as managed security services to customers as shown on the following slide.*
  - MSSPs are just one of many WAF purchasers but offer an interesting perspective on the competitive landscape.
  - MSSPs typically require solutions that are highly scalable, reliable, and provide leading security efficacy.

### Competitive Environment Discussion (continued)

**Web Application Firewall Market: Managed Security Service Provider Ranking**

**North America, 2015**

**Normalized MSSP Ranking**

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5 Web Application Firewall</td>
<td>8</td>
</tr>
<tr>
<td>Imperva Web Application Firewall</td>
<td>7</td>
</tr>
<tr>
<td>Arbor Networks Web Application Firewall</td>
<td>6</td>
</tr>
<tr>
<td>IBM Proventia Web Application Firewall</td>
<td>5</td>
</tr>
<tr>
<td>Trustwave Web Application Firewall</td>
<td>4</td>
</tr>
<tr>
<td>Sophos Web Application Firewall</td>
<td>3</td>
</tr>
<tr>
<td>Fortinet Web Application Firewall</td>
<td>2</td>
</tr>
<tr>
<td>Barracuda Web Application Firewall</td>
<td>1</td>
</tr>
</tbody>
</table>

**Explanation of methodology**

1. The security platforms supported by MSSPs are weighted by MSSP market share to produce aggregate ranking.
2. The aggregate rankings are then normalized on a 10-point scale. “10” represents the most highly used security platform overall.

Source: Frost & Sullivan
## Competitive Factors and Assessment

### Total WAF Market: Competitive Factors and Assessment, Global, 2015

<table>
<thead>
<tr>
<th>Competitive Factor</th>
<th>Customer Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accuracy</strong></td>
<td>• Protection against OWASP Top 10 Threats</td>
</tr>
<tr>
<td></td>
<td>• Low false positive rates with behavior-based detection enabled</td>
</tr>
<tr>
<td></td>
<td>• Third-party testing and certification</td>
</tr>
<tr>
<td><strong>Advanced Features</strong></td>
<td>• Bot detection</td>
</tr>
<tr>
<td></td>
<td>• Device reputation</td>
</tr>
<tr>
<td></td>
<td>• Anti-scraping</td>
</tr>
<tr>
<td></td>
<td>• Fraud detection</td>
</tr>
<tr>
<td></td>
<td>• Web site defacement prevention</td>
</tr>
<tr>
<td></td>
<td>• DDoS detection and mitigation</td>
</tr>
<tr>
<td></td>
<td>• Dynamic Web application profiling</td>
</tr>
<tr>
<td></td>
<td>• Custom/third-party rule sets</td>
</tr>
<tr>
<td><strong>Integration</strong></td>
<td>• WAF integrates with or offered as optional add-on module for ADCs, NGFWs, and CDN services</td>
</tr>
<tr>
<td></td>
<td>• Integration with advanced malware solutions and DDoS mitigation solutions</td>
</tr>
<tr>
<td></td>
<td>• Bi-directional integration with DAST tools (both static and dynamic)</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan
## Competitive Factors and Assessment (continued)

<table>
<thead>
<tr>
<th>Competitive Factor</th>
<th>Customer Requirements</th>
</tr>
</thead>
</table>
| **Usability**      | Out-of-the-box rule sets  
                      | Ease-of-deployment  
                      | Virtual and cloud appliances for protection of applications in all environments  
                      | Managed security services |
| **Scalability**    | Use of purpose-built hardware to accelerate functions such as SSL inspection  
                      | High availability features and fail-open deployment modes  
                      | Minimal impact on end user experience |
| **Cost of ownership** | Product prices  
                       | Lower total cost of ownership  
                       | Requires fewer security experts to deploy and operate |

Source: Frost & Sullivan
Competitive Factors and Assessment Discussion

Accuracy

• The high false positive rates of early WAF products has been a challenge for the market.
  
  o False positive rates can be minimized by disabling rule sets and behavior based detection. However, this compromises the security posture of the Web application.
  
• Ideally, customers should be able to deploy a WAF with full behavioral detection enabled with minimal false positive rates.

• Third-party testing can provide a balanced and impartial approach for customers to determine the accuracy of available WAF solutions.

Source: Frost & Sullivan
Advanced Features

- Early WAFs and integrated WAFs offer basic protection against simple attacks such as SQL injection and cross site scripting.

- However, modern WAFs must provide the functionality to defend against new threats.
  - Advanced features such as bot detection, device reputation and fingerprinting, anti-scraping, fraud detection, Web site defacement prevention, and DDoS mitigation all help to detect more sophisticated attacks, automated attacks, or unwanted devices, bots, and malicious users.

- More technically sophisticated customers may require the ability to create custom rule sets.

- Some features such as dynamic Web application profiling can help to simplify deployment while also improving security.
  - For example, dynamic Web application profiling allows the WAF to analyze and protect Web applications such as identifying pages that might be exploited in “heavy URL” DDoS attacks.

Source: Frost & Sullivan
Integration

• WAF is often considered in relation to other application delivery and security tools such as ADCs, NGFWs, and CDN services.
  
  o The strength of these related products may determine which WAF a customer will invest in.

• Vendors such as Fortinet are integrating WAF data with advanced malware sandboxing solutions to identify advanced threats that can evade point products.

• WAF can aid DDoS mitigation solutions by identifying and stopping application layer attacks. DDoS mitigation solutions that rely solely on network traffic sampling and metadata lack visibility into application layer traffic.
  
  o Security labs report that application layer attacks such as HTTP GET floods and HTTP POST floods are becoming more popular.

• More sophisticated businesses also benefit from bi-directional integration with application security testing tools (both static and dynamic). This integration will enable customers to protect application vulnerabilities with virtual patches until a software patch can be developed and deployed.

Source: Frost & Sullivan
WAF services meet the needs of an underserved and growing market segment.

WAF Service Segment: Revenue Forecast, Global, 2012–2020

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan
WAF Service Segment—Revenue Forecast Discussion

• WAF services provide many advantages over appliances.
  o WAF services replace a large capital investment with a manageable operational expense.
  o WAF services can be deployed quickly, in a matter of hours instead of days or weeks.
  o The price for WAF services include maintenance and support.
  o WAF services are often provided as an add-on to CDN services or include valuable application delivery and acceleration capabilities.

• These benefits allow a previously underserved market segment to deploy WAF capabilities.

• The WAF services segment is limited by free WAF services and value-adding WAF capabilities.
  o Though these services include a very basic type of WAF, this may be adequate protection for smaller businesses.

Source: Frost & Sullivan
WAF Service Segment—Pricing Trends and Forecast

WAF services are steadily increasing in price as vendors penetrate large business accounts.

Average Price for WAF Service Segment: Global, 2012–2020

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan
Service Segment—Pricing Trends and Forecast Discussion

- WAF services cost less than appliances but are a recurring monthly or yearly expense.
  - Entry level WAF services start at a couple hundred dollars per month per Web site.
  - Enterprise subscriptions can cost several thousand dollars depending on the number of Web sites and applications that require protection.
- Additionally, WAF services require less technical expertise to deploy and maintain.
- WAF service contracts also include updates and support in the subscription price.
- Increasing penetration into larger business and enterprise accounts is driving steady growth in average price.

Source: Frost & Sullivan
Akamai has established a leadership position in the WAF services market.

Percent of Revenue
Service Segment: Global, 2015

- Akamai: 62%
- Company A: 9%
- Company B: 6%
- Company C: 3%
- Company D: 3%
- Company E: 1%
- Others: 15%

N=10

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan
Vendor Profile: Akamai
Vendor Profile: Akamai

Company Background

Akamai (NASDAQ: AKAM) is the leading provider of CDN services, including application delivery, acceleration, and security. Akamai Kona Site Defender includes WAF and DDoS mitigation. Akamai solutions protect some of the largest Internet properties in the world.

Revenue Estimates

Total Market: 17%

Geographic Segmentation

Akamai customers are based primarily in the Americas and the company is growing in EMEA and APAC as well.

Delivery and Channel

Akamai has a wide range of technology and reseller partnerships.

Key Differentiators

Akamai maintains one of the largest CDN infrastructures in the world. Akamai manages 200,000 servers in 1,400 partner networks in 110 countries around the world. Akamai estimates it can see up to a third of global Internet traffic. The Akamai Cloud Security Intelligence platform analyzes up to 2 Terabytes (TB) of data and 10 billion Web security events per day.

Source: Frost & Sullivan
Strengthenes and Opportunities

• The Akamai Kona Site Defender solution offers integrated WAF and DDoS mitigation for comprehensive Web site protection.

• Akamai analyzes 2 Petabytes of security data collected from up to 30% of all Web traffic through its Cloud Security Intelligence platform. Akamai used this threat intelligence to develop its own proprietary set of web application protections, which Akamai claims has unrivaled accuracy.

• Akamai offers a premium service called Client Reputation as an add-on for Kona security solutions. Akamai Client Reputation uses behavioral analytics and Akamai threat intelligence to identify and filter traffic from IP addresses that have attacked or abused customer websites.
  o Akamai Client Reputation successfully blocks hundreds of millions of malicious IP addresses monthly.

• Akamai Bot Manager is a new offering that helps customers to enact granular controls over the various bots that visit their sites. Akamai Bot Manager offers identification, classification, and control of all bot types, from benign, helpful bots to pernicious, unwanted bots such as DDoS bots, spammers, scanners, and scrapers.

Source: Frost & Sullivan
Strengths and Opportunities (continued)

- Akamai solutions are managed through the Luna Control Center for centralized and customized visibility and control. Akamai solutions may be supported by Akamai Professional Services experts.

- Additionally, Akamai offers a Managed Security Service based on its Kona solutions. The Akamai Managed Security Service offers a number of features such as a Threat Update Review, Security Configuration Assistance, Table-Top Attack Drills, 24/7 Security Monitoring, Attack Support, Monthly Solution Report, Security After Action Report, and a Managed Security Advocate.

- Akamai security solutions are enhanced by the Akamai Threat Research Division—a team of experts that actively monitor and analyze emerging threats and attack trends.

- Akamai Cloud Security solutions is a high growth product line for the company. Akamai’s cloud services align well with customers’ operational expense models and provide agility to adapt as threats and requirements change.
  - Additionally, Akamai solutions offer customers a comprehensive portfolio of Web delivery, acceleration, and security.
  - Kona Site Defender is a top consideration for Akamai’s thousands of CDN subscribers.

Source: Frost & Sullivan
Vendor Profile: Akamai (continued)

**Weaknesses and Threats**

- In previous years, Akamai has been challenged to quickly adapt and enact new security rules.
  - However, Akamai has updated its architecture to enable rapid updates to DDoS and WAF rule sets when threats are detected.
  - In 2015, Akamai announced a capability for Managed Security Service customers called “Expedited Activation” that allows new WAF rules to be enacted in under a minute. Akamai plans to offer the feature as a self service capability by late 2016.
- Akamai often faces the question of how to inspect encrypted traffic for organizations that are reluctant to share SSL keys with cloud security vendors.
  - To address this, Akamai has developed methods to inspect SSL traffic without the need to share private keys.
  - Akamai has proven capable of handling private keys securely in many enterprise sales. Additionally, all cloud security companies face this same challenge.

Source: Frost & Sullivan
One of Frost & Sullivan’s core deliverables is its Market Engineering studies. They are based on our proprietary Market Engineering Methodology. This approach, developed across the 50 years of experience assessing global markets, applies engineering rigor to the often nebulous art of market forecasting and interpretation.

A detailed description of the methodology can be found here.
About the Author

Chris Rodriguez
Senior Industry Analyst
Frost & Sullivan
North America
San Antonio, TX

Functional Expertise

- Seven years of industry analyst experience including primary research, consulting projects, video presentations, public speaking engagements, and webinars.
- Experience working on special projects including:
  - International expansion go-to-market research and strategy guidance
  - Merger and acquisition due diligence research including SWOT analysis, customer satisfaction review, and new product/new market analysis
  - Distribution channel analysis and guidance including professional introductions

Industry Expertise

- Experience base in the information and communication technologies (ICT) sector, leveraging long-standing relationships with Senior Executives at leading companies in the areas of:
  - Next generation firewall (NGFW) and unified threat management (UTM)
  - Intrusion prevention systems (IPS)
  - Web application firewall (WAF)
  - Distributed denial-of-service (DDoS) mitigation solutions
  - Endpoint security and mobile endpoint protection
  - Vulnerability research and management
  - Network access control (NAC)
  - Identity and access management (IAM)

What I Bring to the Team

- Experience helping Fortune 500/Global 1000 clients with strategic market communication and education initiatives
- Ability to communicate the business value of network security technologies to non-technical decision makers
- Capacity to interact with and provide strategic business intelligence and guidance to C-Level executives

Education

- Bachelor of Science in Computer Information Systems from the University of the Incarnate Word, San Antonio, Texas

Source: Frost & Sullivan
About Frost & Sullivan
Information and Network Security Research Programs

Frost & Sullivan's Network Security Research and Consulting practice provides global industry analysis, custom consulting, growth consulting and market research & forecasts that help your firm grow.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Advanced Persistent Threats (APT) Detection and Mitigation</td>
<td>• Examination of market dynamics</td>
</tr>
<tr>
<td>• Distributed DoS (DDoS) Attack Mitigation</td>
<td>• Creation and presentation of market dimensions</td>
</tr>
<tr>
<td>• Endpoint Protection and Security</td>
<td>• Examination of market participants’ strategic movements</td>
</tr>
<tr>
<td>• Network Forensics</td>
<td>• Creation and presentation of market growth recommendations</td>
</tr>
<tr>
<td>• Identity &amp; Access Management (IAM)</td>
<td>• Advanced Threat Detection and Mitigation</td>
</tr>
<tr>
<td>• Intrusion Detection and Prevention Systems</td>
<td>• Cloud Security</td>
</tr>
<tr>
<td>• Managed and Professional Security Services</td>
<td>• Desktop Virtualization</td>
</tr>
<tr>
<td>• Network Access Control (NAC)</td>
<td>• File Sharing and Synchronization</td>
</tr>
<tr>
<td>• Public Vulnerabilities</td>
<td>• Hardware-embedded Security</td>
</tr>
<tr>
<td>• SIEM and Log Management</td>
<td>• Identity and Access Management (IAM)</td>
</tr>
<tr>
<td>• SSL Certificates</td>
<td>• Identity Assurance and Strong Authentication</td>
</tr>
<tr>
<td>• Strong Authentication</td>
<td>• Network Security Usability</td>
</tr>
<tr>
<td>• Unified Threat Management and Next-Gen FW</td>
<td>• Secure Containerization and MDM</td>
</tr>
<tr>
<td>• Vulnerability Management</td>
<td>• Secure Software Development</td>
</tr>
<tr>
<td>• Web and Email Content Filtering</td>
<td>• Software Defined Networking (SDN)</td>
</tr>
<tr>
<td>• Web Application Firewall (WAF)</td>
<td>• Tokenization</td>
</tr>
</tbody>
</table>
Legal Disclaimer

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers’ internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041