

Web Application Firewalls:
Application Protection and Much More

Business Market Strategies, Volume 1, Number 13



WEB APPLICATION FIREWALLS: APPLICATION PROTECTION AND MUCH MORE

Business Market Strategies
Volume 1, Number 13

EXECUTIVE SUMMARY

The Web Application Firewall market as it existed several years ago has disappeared. The Web Application Firewall of yesterday has been superseded by a new generation of Web Application Firewall that not only delivers enhanced security features, but also provides more sophisticated features to appeal to large enterprises. Advanced security features include learning modes, customized security policies, sophisticated correlation algorithms, improved policy management, and more. In addition to these enhanced security features, vendors have also developed systems that integrate features that appeal to large enterprises such as availability, scalability, high performance, traffic management, and endpoint security management.

Stratecast believes that the evolution of the security market in general, and the WAF market specifically, will continue and will deliver stronger products enabling more secure deployments of applications. It is likely that acquisitions will continue, most likely the pure play vendors; that the number of threats will increase, particularly with the development of Web 2.0 and more sophisticated AJAX applications; and that Web Application Firewalls will become an integral part of a unified approach to security.

INTRODUCTION¹

The natural evolutionary process of the IT market dictates that products change to accommodate new market demands. And over the past several years, the information security market has dramatically reflected that evolutionary change. Originally the market demanded protection against threats such as unauthorized network access and malicious code, and vendors delivered products such as anti-virus software, network firewalls, VPNs, and intrusion prevention/detection systems (IPS/IDS), among others. Today, as the result of technology changes (particularly the Internet) and changes in business processes, we are witnessing a new phase of evolution in the information security market.

Internet technology has given enterprises new opportunities to improve productivity, lower costs, increase revenues, and maintain closer relations with customers and trading partners. However, simultaneously it has opened the door to increased risk and threats to the enterprises' most valuable resources—their data. Many organizations believe their data is

1. In preparing this report, Stratecast conducted interviews with representatives of several notable Web Application Firewall Vendors.

Please note that the insights and opinions expressed in this assessment are those of Stratecast and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

protected because they have a network firewall, or have implemented IPS/IDS or anti-virus software, not realizing these traditional security products do not protect against Web application attacks and, in some instances, do not even recognize them as threats.

Although Web Application Firewalls (WAFs) represent a mature market, their demand is increasing and they are becoming an integral part of many enterprises' broader and more unified approach to information security. In so doing, they will play an important part in the next evolutionary phase of the information security market.

THE PLACE FOR WAFs IN THE SECURITY PUZZLE

An increasing number of businesses rely on Web-based applications as an essential component of their business critical application processing, through activities such as supplier collaboration, inventory management, online sales, and customer account management. These activities have demonstrated improved efficiencies, cost reductions, and increased revenues and profits. However, Web applications have also given hackers and professional data thieves the opportunity to exploit application vulnerabilities and do serious corporate damage by stealing enterprises' most sensitive information, such as financial records, credit card numbers, and customer information.

In the past, customer-, application- and employee-data resided in the data center behind a company's network firewall. But today, legitimate application behaviors, such as port hopping and tunneling, allow applications to find open ports in a firewall—making it nearly impossible for traditional security devices operating at layer 3 to detect potential threats in those applications.

And with the collaborative environment in which Web applications function, they routinely and unhesitatingly take practically any type of input, assume that it's valid, and process it further. Not validating input is one of the greatest mistakes that Web-application developers can make. This lapse in security planning can lead to system crashes, malicious database manipulation and even database corruption, and data theft.

Obviously one answer to protect against these application attacks is to ensure that Web applications are securely coded; however, business pressures usually require that applications be delivered as quickly as possible, thus reducing the security testing cycle. A more expedient solution is the deployment of a Web application firewalls. WAFs have been effectively protecting Web applications from both internal and external malicious attacks for several years. Even so, each vendor in the WAF marketplace is taking a different approach in its WAF development and delivery.

The purpose of this research paper is to clarify the purpose of WAFs and the different approaches the major vendors are taking. To accomplish that, this paper will discuss how Web Application Firewalls can protect enterprise data against Web-based threats and how they differ from traditional network layer firewalls. It will also demonstrate that WAFs are an important element in the next phase of the information security market's evolutionary process, and discuss how that next phase demonstrates the role that WAFs can play as part of an enterprise's unified threat management environment. Also contained in this paper we

will discuss what type of organizations can benefit from WAF implementation, what criteria can be used to evaluate WAFs. We will end with analyzing the offerings of seven major vendors in the Web Application Firewall market, and discuss their strategy for security in the next evolutionary phase of the market.

WEB APPLICATION FIREWALLS: TECHNOLOGY AND MARKETS

Web Application Firewalls are network devices that operate in front of business-critical Web-, application-, and database-servers. WAFs grew out of the awareness of enterprises and Web application developers that these new applications opened up a huge vulnerability for hackers to steal corporations' most essential data—its customer and corporate information including account numbers, personal data, social security numbers, financial or medical information, and inventory data.

WAFs operate on data at layer 7 of the OSI reference model and protect Web servers from attacks. They act on browser and HTTP attacks that try to manipulate application behavior for malicious purposes, and look for violations in application-specific policy. Typically they enforce security policies at a very granular level by building a model of the manner in which users interact with the application and preventing traffic that does not adhere to that model. This model is called the positive security model.

In contrast, traditional network firewalls, IPsec VPNs, and intrusion prevention/detection systems (IPS/IDS) operate at layer 3, and in most organizations are the first line of defense against intruders. They perform functions such as validating the format of application header data, blocking unauthorized network-level requests, limiting access to specific ports, and managing network access control. Typically, attacks against the network layer 3 are designed to impact availability, and in fact many people consider them nuisance attacks. However, with application attacks, hackers discover application vulnerabilities with a view toward stealing corporate customer data (e.g., accounts numbers, and social security numbers), disrupting business processes, and potentially causing serious financial and legal problems.

Over the years, the architectural basis of Web application firewalls has changed from deep-packet inspection to a proxy-based design. Although the deep-packet option provides better performance, the proxy-based architectures better accommodate increasing complexity of today's security policies. A proxy functions as a relay between client and server, terminating incoming TCP, SSL, and HTTP protocols to provide visibility into the application. This termination capability gives the proxy the opportunity to inspect the entire session payload including not just headers, but also URLs, buttons, form fields, and parameters. Bi-directional proxies evaluate not just incoming traffic, but also protocols and requests to the Internet. All of the vendors in this study employ proxy technology with the exception of Breach Security with its WebDefend product and Microsoft, with ISA Server. However, Breach's recently acquired ModSecurity offers a reverse proxy design, and Microsoft's Whale Intelligent Gateway is an SSL proxy. Some vendors such as NetContinuum and Imperva support deployment of a proxy but do not require it.

Most Web application firewalls are sold in the financial services, healthcare, application service provider, and e-commerce business segments. These environments typically host highly sensitive data such as customer account information, credit card numbers, medical information, or financial data. Any organization that requires high availability services or enables transactions that exchange sensitive data can benefit from a WAF. Typically, those enterprises that maintain primarily informational Websites do not have need for a Web application firewall.

WAFs vs. Layer 3 Devices

WAFs address different issues than network firewalls and layer 3 devices. They require an understanding of application threats and of application functionality, and must prevent abuse from external and internal users. That means that Web application firewalls protect application data from identity theft and also from malicious behavior by authorized users, while simultaneously enabling application access for legitimate users.

Although network firewalls and IPS/IDS do provide some application layer protection, they cannot protect against more sophisticated Web application attacks such as SQL injection, URL tampering, or cross-site scripting, among others. Layer 3 devices can enforce compliance of protocols associated with the application layer (e.g., http: for Web traffic; SMTP: for mail), and they may also detect easily identifiable attacks by looking for attack signatures in an HTTP header, but they do not provide the same level of inspection that WAFs do.

Devices, such as network firewalls, that evaluate IP packets or protocols, without an awareness of the application payload cannot provide application protection. For example, IP packet inspection will not recognize a hacker who has changed the session ID in a URL line to access another person's data; or someone who has compromised a session cookie to assume another person's identity. Without an awareness of the HTML data payload these layer 3 devices cannot recognize and overcome these types of application layer threats. Web application firewalls can detect the injection of malicious scripts in HTML form fields, and prevent a cross-site scripting attack, which can access cookies, session tokens or sensitive information held in a browser.

Some organizations believe that because they employ SSL their data is protected. Although SSL does provide a level of security, and is necessary to transmit information securely, it does not secure Web applications. SSL protects data during transmission, but not at the end points, and in fact it gives application hackers a means to avoid detection. Hackers can use an SSL-encrypted session to launch an attack against a Web application because the SSL tunnel hides the malicious attack.

Newer Generation of WAFs

The newer generation of Web application firewalls has improved significantly from those marketed several years ago. Today the new generation firewalls employ both a negative and positive security model, as described below, and many also provide security policy learning modes, sophisticated event correlation, and customized security policies.

- **The negative security model specifies known bad traffic.** In this model, attacks are recognized and blocked by relying on a database of known attack signatures. Anti-virus and intrusion detection/prevention systems are classic examples of the negative security model. This type of model provides limited protection against new attacks.
- **A positive security model specifies known good traffic.** This model focuses on those actions that are allowed, and prevents those that are not allowed. This model is very effective at preventing unknown attacks. Some new generation WAFs create a positive security model of application usage that includes URLs, parameters, hidden fields, and session IDs. They compare these attributes to the security model and block them if they do not conform.
- **Learning mode monitors and evaluates the production traffic to learn acceptable application behavior.** The software then recognizes malicious behavior, such as patterns that match social security numbers, and blocks the request. This feature gives organizations the opportunity to customize their security rules for specific applications.
- **Some products allow security administrators to define and customize policies related to specific application behavior.** This gives organizations the opportunity to perform activities that are not easily implemented via profile and protocol violation rules.
- **Sometimes suspicious activity cannot be classified as good or bad.** Therefore, some vendors, notably Imperva, have developed algorithms that correlate suspicious activity and violations across multiple applications and over time to identify violations from legitimate activities.
- **Endpoint security management.** Policies make it possible to define several levels of trust for each user. Companies may want to enable some form of access, even if a user cannot accept all desired forms of remote protection. For example, granting limited on-demand access may be more important for convenience, emergencies and business continuity than a traditional security approach, which would deny anything but a perfectly crafted connection.

WAFs and Enterprise-Grade Attributes

This new generation of Web application firewall represents a critical component in the next phase of the evolutionary trend in data center security. Although many new features have been added to next-generation WAFs, as described above, other important enterprise-grade attributes reside in add-on boxes that become part of an integrated or unified threat management system. These enterprise-grade capabilities include features to:

- enhance performance,
- reduce latency (accelerate responsiveness),
- improve availability and scalability, and
- integrate and simplify management.

Although many of the vendors outlined in this report offer these features, the providers' strength usually reflects the industry background from which they come. For example, some WAF providers have long histories in the security market, but have added acceleration capabilities to their product portfolio—typically their strength reflects the security background. Similarly, other vendors have strong experience and depth in system uptime or traffic management and are relatively new entrants to the security market—typically their strength lies in availability or acceleration. In each of these cases, during the purchasing process, the strengths of each vendor and the demands of the enterprise should be weighed and balanced.

Figure 1: WAF Enterprise-Grade Attributes

Attributes	Description
Performance Enhancements	<p>Web applications are designed to handle high throughput and high transaction rates. But to measure these high-throughput rates, users should evaluate HTTP transaction rates and latency under realistic transaction processing scenarios including a full production simulation with functions such as URL requests, layer 7 ACLs (access control lists), and dynamic application profiling. To achieve these high throughput rates, each vendor has implemented performance improvements in different ways.</p> <p>What follows are some of the methods that select vendors have chosen. For example, Imperva does security processing at the kernel level, which requires less processing overhead. NetContinuum terminates all protocols and application functions within its custom operating system, NCOS; and F5 has written an operating system, TMOS, that does many of the full proxy capabilities at line rate. Citrix offloads compute- and memory-intensive TCP connection management from Web servers, and employs dedicated SSL hardware to detect malicious code in encrypted tunnels. These represent only some of the methods employed in each product portfolio.</p>
Acceleration	<p>Vendors have also incorporated acceleration features either in their WAFs or as add-ons. These acceleration features include functions such as TCP pooling, which minimizes the number of TCP handshakes between the proxy server and backend application server by re-using open TCP connections between those devices. Nearly all vendors employ page compression algorithms to reduce bandwidth consumption and accelerate page downloads. Some compress encrypted and unencrypted data in real-time; and some proxies offload GZIP compression from the application servers to save CPU cycle times. Dynamic caching is also used in conjunction with compression to accelerate traffic. For example, F5 and Citrix have a dynamic caching feature that looks at the application logic and behavior, and by understanding an application's logic it can eliminate repeated processing of complex Web requests.</p>

Availability and Scalability

Since Web applications are so tightly tied to revenue and productivity today, any downtime costs money in terms of reduced customer satisfaction and employee efficiency. Therefore, availability is becoming an increasingly important function for WAFs. Typically, those vendors that entered the security market from the traffic management or system uptime market segments provide more sophisticated and robust availability features. Nevertheless, today nearly all vendors offer availability features either integrated into their product line or through partnerships. In some cases, vendors improved availability by simplifying deployment; in other cases they have integrated sophisticated load balancing features. For example, NetContinuum offers a bridge deployment option, which obviates the need for network architecture changes including routers or load balancers. Imperva, with its SecureSphere WAF, supports a wide range of availability features. For example, Imperva can deploy redundant gateways in environments with redundant system infrastructures, and also provides for inline fail-open network interfaces to ensure availability if hardware or software fails. F5, representing its depth of experience in traffic management, delivers a Global Traffic Manager product that monitors the health of the infrastructure to prevent single points of failure and to route traffic away from poor performing sites. It also aggregates multiple health checks so enterprises can check application availability at multiple levels. Global Traffic Manager also checks the health of applications that are dependent on one another in order to build scalable traffic distribution policies.

Vendors also provide varying degrees of sophistication in load balancing to improve availability. For example, NetContinuum load balances FTP traffic between back-end servers using several different load-balancing algorithms. F5, with its BIG-IP Global Traffic Manager, can resolve IP addresses to the country level in order to effectively manage global traffic. And Citrix's Global Server Load Balancing option directs traffic to the site that is best able to fulfill the client's request based on site availability and capacity. In multi-site application environments, Citrix also redirects user requests to the available data center most likely to fulfill the request. This is further enhanced by Citrix's flexible deployment model, which enables clusters of application firewalls to scale linearly with additional box count while centrally managing all of the boxes in the cluster.

Management

The combination of the increasing complexity of network infrastructures and applications, the increasing number of security devices, the complexity of enforcing security policies, and the demands placed on the security system by regulatory requirements force enterprises to compare management options. Each of the WAF vendors offers capabilities relative to managing the security environment, ranging from simple logging and reporting to a centralized management server that can be used as part of a unified threat management environment. For example, Imperva's MX Management Server manages multiple gateways centrally and aggregates policy, monitoring, and logging across those gateways. Secure Computing's Sidewinder Enterprise Manager is a security appliance that delivers centralized policy management and audit logs for Sidewinder's distributed security appliances. Breach Security has developed APIs that enable the WebDefend system to interoperate with other management environments, such as WebSphere. Microsoft, with its ISA Server, gathers data from logs, configuration profiles, and publishes that data for reporting to management. Microsoft does not produce SNMP data that third-party management systems, such as OpenView, can read.

Source: Stratcast

Types of Application Attacks

The Open Web Application Security Project (www.owasp.org) is a non-commercial, independent organization established to develop and distribute information related to application security. As part of its work, it has created a list of the top ten Web application security vulnerabilities. A brief description of vulnerability examples related to input, access control, and availability are described in the table that follows to demonstrate differences from layer 3-related attacks.

Figure 2: Types of Application Attacks

Application Attacks	Description
Input Attacks	Several varieties of input attacks against Web applications have been identified by OWASP. This type of attack typically inserts malformed data into a packet, which can enable the application to share too much information with the attacker. Buffer overflows, for example, target input fields in Web applications. If those fields are not properly validated, the hacker can take control of a process, or can crash the system. Code injection attacks (e.g., SQL Injection) enable the hacker to modify the URL in the client browser before the data is returned to the server and thus attack backend components. Almost all external calls (e.g., system calls, SQL requests, shell commands) can be attacked if the Web application is not properly coded. Cross-site scripting vulnerabilities, another type of input validation attack, occur when an attacker uses a Web application to send malicious code to another user. Because the end user's browser believes the script arrived from a trusted source, the malicious script can access cookies, session tokens, or other sensitive information held by the browser.
Access Control Attacks	Access control or authorization enables Web applications to grant access to specific content or to functions only to authorized users. However, in a broken access control vulnerability, restrictions on unauthorized users are not adequately enforced. This gives hackers the opportunity to view confidential files or use unauthorized functions. Since a Web application's access control model is so integrally linked to the content and functions that the site provides, it is typically difficult to implement properly, and thus likely for potential attack.
Availability Attacks	Denial of service attacks is a well-known vulnerability that inhibits system availability. With this type of attack, a hacker can generate such high volumes of traffic from a single host to inundate some applications. If the attacker can consume all of a system resource, such as disk storage, database connections, threads, and bandwidth, legitimate users are prevented from using the applications. (Please note that this type of Web application denial of service attack is different from network denial of service attacks, such as SYN floods).

Source: Stratecast

Choosing a WAF

Considering the potential loss that can occur if a Web application is breached and corporate data is stolen, the reasons for investing in a WAF are becoming much better recognized by enterprises. However, methods for evaluating the WAF deployment can be difficult. Because of the increasing complexity of next-generation WAFs and because of the variety of enterprise requirements, no single WAF is appropriate for all networks, and there is no single checklist that all organizations can use to indicate must-have features. Rather, each enterprise must recognize their business goals and identify the security required from

a WAF investment. For example, some enterprises may demand a high degree of HTTP level performance, others require strong protection of XML Web services, others may demand strong detection techniques, and e-commerce companies must insure PCI compliance. To help with product evaluation and selection, the Web Application Security Consortium (www.webappsec.org), an international group that produces best practices security standards for the Web, has developed a set of WAF evaluation criteria and testing methodology. Stratecast recommends that WAF purchasers thoroughly review all WASC criteria before considering a Web Application Firewall investment.

MARKET DEMAND OVERVIEW

A number of market, technology, and regulatory factors have coalesced to make the enterprise IT and security professional's job even more difficult than in the past. Today, more and more organizations are relying on Web-based applications to improve productivity by collaborating with trading partners, by providing customers with self-service and account management options, and by enabling and supporting more telecommuting. This collaboration and transparency has contributed to improved corporate efficiencies and productivity. However, simultaneously the opportunity for hackers to do serious financial damage to a corporation's business critical resources has increased dramatically. A successful hack can jeopardize not only Web and application servers, but also database servers, which hold business critical customer and enterprise information. A number of enterprises are also seriously evaluating WAFs to obviate the possibility of being held hostage by a hacker who threatens to bring down a Web site unless a ransom is paid.

At the same time that the market has been evolving, enterprises and users have recognized the dangers that this new transparent and collaborative approach to business process can bring to the organization. Many enterprises have recognized that their layer 3 network firewall, IPsec VPN, and intrusion detection/ prevention systems cannot protect against abuse of their Web applications and have looked for alternatives to solve the new application security problems. In addition, many enterprises (and vendors) are also now anticipating how to protect against evolving technology changes such as Web 2.0, with its promise of greater interconnectivity, and high-level scripting languages such as AJAX (Asynchronous JavaScript and XML), with its ability to offer richer Internet applications.

Finally, according the 2006 CSI/FBI (Computer Security Institute/FBI) survey, the second most critical security issue for the next two years is policy and regulatory compliance, specifically for Sarbanes-Oxley and HIPAA (Health Insurance Portability and Accountability Act). These regulations represent just two of the several government and industry-based standards that enterprises face. Sarbanes-Oxley mandates that the CIO is responsible for security, accuracy, and reliability of the systems that manage and report financial data. HIPAA dictates that medical facilities must perform security testing to provide a baseline security review of all computer systems. The Gramm-Leach-Bliley Act (GLB) requires that a policy must be in place to protect information from security and data integrity threats. And, the recently updated PCI-DSS (Payment Card Industry-Data Security Standard) industry standard mandates use of an application firewall—representing an excellent sign

that the industry recognizes the value of a Web application firewall. The goal of the PCI standard, which was introduced by MasterCard, Visa, American Express, and JCB, is to eliminate debit and credit card fraud among merchants by dictating how cardholder data is handled and protected. Although regulatory compliance is a critical issue for security professional, the use of a WAF does not guarantee compliance. In many cases enterprises use WAFs for assurance purposes and to show log files to auditors and demonstrate proactive measures that are taken to protect data. Some vendors, such as Secure Computing with its Sidewinder Security Reporter product, facilitate compliance with HIPAA, Sarbanes-Oxley, and GLB.

As a result of these market, technology, and regulatory drivers, both hardware and software vendors have seen the demand for Web applications rise over the past several years. Based on responses to the 2006 CSI/FBI survey, Stratecast believes that demand will continue. According to the survey, respondents ranked data protection and application vulnerability security as the most critical security issues they expect to face over the next two years. This result, in combination with the survey results that only 39% of respondents employ an application firewall, points to a positive growth for the WAF market. Although demand will likely increase, it is uncertain what type of WAF enterprises will choose. Options range from a standalone, best-of-breed appliance, to an integrated approach that offers additional features such as database security, application delivery control, and application traffic management. The choice depends on the business demands of the enterprise. Some organizations may require strong attack protection; others may value ease of use, high-performance or global load balancing capabilities; and others may opt to add application security from the vendor that already provides their network devices.

The Future of WAFs

In keeping with the evolutionary trend of the marketplace, acquisitions will certainly continue into the future. It is very likely that some of the pure-play WAF providers will be subsumed by other vendors, particularly those network or acceleration-based vendors who may enter the security market. These will complement the acquisitions that have occurred in the recent past such as Microsoft's acquisition of Whale Communications, F5's purchase of the MagniFire Web application firewall and WatchFire's AppShield WAF, and Citrix's acquisition of Teros. At the same time, multifunction security providers will continue to enhance performance, availability, and acceleration functions, and add more security capabilities in order to become stronger players in the evolving unified threat management space.

From a technology perspective, two technologies, specifically Web 2.0 and AJAX, will become more prevalent and precipitate more targeted application attacks. Web 2.0 represents the evolution of the Web and is a transition from the Web as a collection of individual Websites to a computing platform that serves Web applications to end users.² AJAX, although not a new technology, is becoming very important to developers and companies because of its capability to create richer interactive Web pages and improve the

2. For additional discussion on Web 2.0, see "Web 2.0 and Internet Revenue Opportunities" (SPIE 6-37) September 29, 2006. Please contact your Account Executive about receiving this SPIE or send an e-mail to inquiries@stratecast.com or call 877-463-7678.

user experience. It is very likely that Web 2.0 and AJAX technologies will increase in usage and, as a result, lead to an increased in the level of security vulnerabilities. The Open Web Application Security Project (OWASP) has already identified Web 2.0 attack vectors. For example, cross-site scripting in AJAX executes malicious JavaScript from a Web site on a victim's browser to compromise information there [not sure of what you wanted]. XML poisoning is another Web 2.0 threat in which attackers produce malformed XML documents coming from AJAX clients, which can disrupt the business logic of the application.

REVIEW OF F5 NETWORKS

Stratecast reviewed several notable Web Application Firewall vendors. A subset of these vendors focus exclusively on the Web application firewall security market. Others have developed a convergence strategy that makes their products part of a unified threat management environment. These vendors have added acceleration and load balancing capabilities to their WAF products to improve performance. A final category of providers offer full stack protection for database-, application-, and Web-servers. This paper will help clarify these strategies.

F5 Networks

F5 has a long and strong reputation as a provider of traffic management, content inspection, and availability products. However, its make-or-break decision on rewriting its OS in 2002 set the company's long-term strategic direction and laid the groundwork for its current integrated product line. At that time, they began rewriting their infrastructure with an eye to providing a modular approach to application security, optimization, and availability.

As a result of this development effort, it introduced in 2004 its TMOS real-time, event-driven, modular operating system that forms the foundation for all its products going forward. F5 claims TMOS combines the performance of a packet-based solution and the intelligence of a proxy solution. It provides a full proxy to intercept and inspect application level content, and claims performance rates that enable the proxy to perform many of the function at line rate.

F5's acquisition of the MagniFire Web application firewall in 2004, the subsequent acquisition of WatchFire's AppShield Web application security technology in May 2005, and its integration with the MagniFire WAF propelled F5 into a leadership position in both the WAF and application delivery marketplaces. Its newly re-branded BIG-IP Application Security Manager (ASM), formerly TrafficShield, implements both a positive security model for dynamic application protection, as well as a strong signature-based negative security model to permit authorized application functions and to provide protection against the OWASP Top Ten vulnerabilities and the WebAppSec Threat Classification lists. The ASM module also leverages F5's TMOS architecture, benefiting from TMOS advantages such as optimized TCP, DOS protection, and flexible iRules, which can make decisions in any layer based on the payload. Application Security Manager uses the back-end applications' business logic to build a usage model to understand all the potential interactions between users and applications. By modeling acceptable application interactions, ASM can then block attempts to deviate from business application policy.

As a result of its F5's long-term strategic decisions and the development of an integrated product line, the vendor maintains a thought-leadership position in the market. The modular design of its BIG-IP product line provides good opportunity to tap into F5's large customer base and cross-sell and up-sell its security, availability, and optimization products on its shared-services platform. The company cannot be complacent in the market as competitors may outwardly question F5's application security experience. In our view, F5 is a serious near-term candidate to capture a large share of the WAF market and its product vision will serve to enhance its position in the longer term.

Stratecast

The Last Word

The profile of the security market has changed over the past several years due to the evolution in business processes, technology enhancements, and increased requirements to protect corporate and individual data. Web application firewalls have grown out of the demand for increased usage of Web applications and from the awareness that network-layer security technologies do not protect applications from all types of hacker threats. As a result, several generations of Web application firewalls have come to market and, through acquisitions and technology advancements, each generation has improved on its predecessor.

This improvement has added much more than just advanced security features such as learning modes, customized security policies, sophisticated correlation algorithms, improved policy management, and more. In addition to these enhanced security features, vendors have also developed systems that integrate features that appeal to large enterprises such as availability, scalability, high performance, and traffic management.

Stratecast believes that the evolution of the security market in general, and the WAF market specifically, will continue and will deliver stronger products enabling more secure applications. It is likely that acquisitions will continue, most likely the pure play vendors; that the number of threats will increase, particularly with the development of Web 2.0 and more sophisticated AJAX applications; and that Web Application Firewalls will become an integral part of a unified approach to security.

Gerald Arcuri
Principal Analyst

Michael Suby
Program Director - Business Market Strategies
Stratecast (a Division of Frost & Sullivan)
msuby@stratecast.com

CONTACT US

Bangalore

Bangkok

Beijing

Buenos Aires

Cape Town

Chennai

Delhi

Dubai

Frankfurt

Kuala Lumpur

London

Mexico City

Mumbai

New York

Oxford

Palo Alto

Paris

San Antonio

Sao Paulo

Seoul

Shanghai

Singapore

Sydney

Tokyo

Toronto

Palo Alto

2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio

7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London

4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost

myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Based in Palo Alto, California, Frost & Sullivan is a global leader in strategic growth consulting. This paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based on research and interviews conducted solely by Frost & Sullivan and therefore is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users.

This publication may not be downloaded, displayed, printed, or reproduced other than for noncommercial individual reference or private use within your organization, and thereafter it may not be recopied, reproduced or otherwise redistributed. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.

For information regarding permission, write:

Frost & Sullivan
2400 Geng Rd., Suite 201
Palo Alto, CA 943033331, USA