POSITIVE TECHNOLOGIES

A SMARTER APPROACH TO APPLICATION SECURITY

Safeguard your business with modern technologies

Issue 2

1
A Smarter and Simpler Approach to Application Security

5
From the Gartner Files: Web Application Firewalls Are Worth the Investment for Enterprises

13
About Positive Technologies

Featuring research from Gartner

Almost every enterprise uses hundreds if not thousands of network, Web, mobile, ERP and client server applications to help run their operations, with new ones popping up almost daily. Your organization must react quickly in response to the ever growing demands of your customers and employees, but as your number of applications grows so too do the number of security vulnerabilities that could be exploited to damage your business.

The Verizon 2014 Data Breach Investigation Report (DBIR) shows that last year 35% of security breaches involved attacks against web applications, up 14% from 2012. The DBIR further concluded that Web app attacks were the most common cause of a data breach, ahead of cyber-espionage, POS intrusion and insider misuse.

Consider this: Positive Technologies recently concluded a series of penetration tests for several large companies. Our experts were able to gain full control over the critical resources of 86% of information systems tested – including payment, email, personal data, ERP (including SAP) and industrial control systems.

The data from these two studies fully supports the fact that data breaches and security incidents are on the rise.

So why are most organizations failing so badly when it comes to application security?

Traditional firewalls and intrusion prevention systems (IPS) no longer provide adequate protection against application-level attacks. Also, most existing application security testing tools are difficult to use and require extensive knowledge concerning vulnerabilities and exploits. Intruders now have highly-automated tools available, allowing them to launch very sophisticated and well-organized attacks that most application protection tools are not ready to face.

TIME FOR A CHANGE

A seemingly logical approach to confronting these new security challenges would be to eliminate as many application vulnerabilities as possible during the software development lifecycle (SDL). In theory, this type of approach should save businesses significant time and money securing their applications, since fixing weaknesses in the design (coding) phase is five times less expensive than doing it in the development stage and exponentially less than in the operation and maintenance phases.

However, experience has proven that implementing secure SDL (SSDL) is expensive and relatively ineffective, due in large part to the inadequacies of existing application security testing tools.

While new automated security solutions could reduce the costs, this would require a common language be agreed to by various departments (development, QA, security check, deployment) involved in the software lifecycle.

Complicating things further, each department involved in an SDL has unique requirements. As a practical example, developers need tools to detect vulnerabilities early in the design process, within the source code. However, to QA, integration with Application Lifecycle Management systems are vitally important, and security pros, who inspect and maintain applications, require easy-to-understand test results with minimal false positives, since they cannot distinguish vulnerabilities from coding errors in some cases.

Making matters even worse, developers are merely focused on applications written in-house, while security personnel must be concerned with the protection of all applications in use, including third-party components that can cause serious problems (e.g., OpenSLL Heartbleed vulnerability).

Many SSDL tools only provide help for applications under development and ignore the reality that an application spends the majority of its life in operation, where risk management is most challenging. Therefore, SSDL solutions cannot protect organizations that rely on third party applications since they cannot control or influence fixing any vulnerabilities they may find. Clearly, there is no "quick fix" or "one size fits all" when it comes to application security. Fortunately, there are some promising new technologies and methodologies for Application Security Testing (AST) and Web Application Firewalls (WAFs) that can simplify the aforementioned difficulties and provide a higher level of security.

A NEW APPROACH TO SAST, DAST AND IAST

Application security testing is commonly divided into static and dynamic analysis. Performed while an application is running from the outside in, much like a black-box, Dynamic Application Security Testing (DAST) is the most simple and widespread method of vulnerability testing. Static Application Security Testing (SAST), on the other hand, analyzes source code from the inside out.

While both traditional methods are useful in finding weaknesses, they each have serious drawbacks. DAST requires applications be deployed for testing and therefore cannot be used when writing code. This method requires that the application be completed, then tested and fixed, which can take a long time and add considerable expense for a large application. Also, DAST cannot detect certain attack vectors, since it can only analyze about 30% of the actual application code. And while SAST allows applications to be inspected at the source code level, it cannot detect vulnerabilities that are only present when an application is running. Worse yet, SAST results are typically plagued with programming errors (not actual vulnerabilities) which generates a high rate of false positives.

These shortcomings and others have led to a hybrid testing approach called Interactive Application Security Testing (IAST). Unfortunately, simply combining SAST and DAST together, as this method suggests, does not eliminate the above-mentioned problems and therefore IAST suffers from the same inadequacies as the others did separately.

But what if you could combine the benefits of traditional static and dynamic analysis without suffering with the downsides? You can.

Positive Technologies Application Inspector™ employs modern science to combine static analysis with partial or full program execution by using symbolic calculations and interactive tracing on part of an application in

a virtual sandbox. This allows the processing of dynamic dependencies, opening functions and classes specific to certain libraries and frameworks, and modeling data flows in a scheme that follows the application logic.

Application Inspector also lets you analyze both partial code as well as compiled-and-deployed applications. It drastically minimizes the number of false positives due to wide source code coverage and context allowance, so your security team can more quickly respond to the real dangers.

SEE HOW YOU'RE BEING EXPLOITED

One new capability to help protect applications is the automatic generation of exploits - special requests that show exactly how an attacker can use a weakness and what data can "activate" it. Originating from the scientific and research community, automatic exploit generation is now available in Positive Technologies Application Inspector providing your security team with one - click capability to see how vulnerabilities found in your applications can be used to attack your business.

As an added benefit, these generated exploits can simplify the practice of secure development, create a benchmark of test cases for QA and be used to train an application firewall, all without the expense of manual code checking and policy development required by other methods.

STOP ZERO-DAY ATTACKS BEFORE THEY START

Today, attackers often exploit zero-day vulnerabilities, making signature analysis obsolete and confirming the need for adaptive solutions that can analyze traffic and maintain statistical models based on normal use patterns. Many corporate applications use highly customized solutions containing third-party code segments and home-grown vulnerabilities. To protect such an application, you need to perform in-depth analysis of interactions between this application and users. Widespread use of robots (fraud, brute-force, botnets, DDoS) also makes it necessary to be able to detect threats in real-time, without prior knowledge of them.

Positive Technologies Application Firewall™ protects web portals, ERP systems and mobile applications against zero-day attacks, web-fraud and data leakage with an innovative use of normalization, heuristics, automatic policy learning and behavioral analysis techniques. With Application Firewall, you spend far less time and money due to shorter remediation cycles.

Integration can be used as an additional method of security tools training. For example, methods of active and passive security analysis built into Positive Technologies Application Firewall allow you to see vulnerable components, libraries and CMSs, and automatically activate the corresponding protection rules.

CONTINUOUSLY FILTER AND RANK THREATS

Modern protection systems (VA/SCA, SIEM, WAF, etc.) have to deal with an enormous number of security events and incidents. An application firewall, for example, typically reacts to thousands of suspicious incidents, which must then be studied in order to find and prioritize threats.

Positive Technologies Application Firewall continuously filters and ranks security events providing a prioritized list of the most critical threats. Built-in correlation provides aggregation, classification and prioritization of threats and analysis of attack chains. Instead of being overwhelmed by thousands of potential attacks, your security team can now focus on and respond more quickly to the most dangerous threats.

It is also worth noting that various application security tools should be integrated into a single ecosystem when possible. Why? By way of example, if an application firewall can exchange information with a code analysis tool, then a potential vulnerability revealed during web traffic analysis could be automatically determined to be a false positive or a true threat. In addition, interaction with DLP and antivirus programs could allow the application firewall to not only detect separate attacks, but also track the attack chain as it develops (e.g., distribution of malicious programs, information leakage, etc.).

RAPID PROTECTION

Experience has shown that many times not even well-known vulnerabilities can be eliminated quickly. Modifying or rewriting code takes resources and time and in some instances requires business critical applications to be offline to fix. Repairing an ERP and e-banking system can take months and hackers know this. A modern application security system should have a mechanism to block security holes without having to wait weeks

or even months for developers to fix them. What if you could create a virtual patch to instantly defend your deployed applications? Deploying both Positive Technologies Application Inspector and Application Firewall allows you to do just that, and more. Application Firewall generates a virtual patch by leveraging Application Inspector's exploit generation capabilities or scans from third-party code analysis tools.

With features not found in other solutions, Positive Technologies MaxPatrol™, Application Firewall and Application Inspector provide a comprehensive and modern answer to today's application security challenges. Their combined power allows organizations to stop fraud and sensitive data leakage and to prevent the collapse of networks and services.

Find all known vulnerabilities across all your applications. Stop zero-day attacks before they strike. Quickly patch existing security holes. See precisely how vulnerabilities can be used to attack your business. Significantly accelerate your incident response and remediation times. And do all of this while drastically reducing your costs associated with compliance.

Now that's a smarter approach to application security.

Source: Positive Technologies

From the Gartner Files:

Web Application Firewalls Are Worth the Investment for Enterprises

Firewalls and intrusion prevention systems don't provide sufficient protections for most public-facing websites or internal business-critical and custom Web applications. Here, we explain how Web application firewalls help security leaders to better protect Web applications in their organizations.

Key Findings

- Web application firewalls (WAFs) are different from next-generation firewalls (NGFWs) and intrusion prevention systems (IPSs). WAFs protect, at a granular level, the enterprise's custom Web applications against Web attacks.
- Even when NGFWs and IPSs are deployed, the WAF is most often the only technology that inspects encrypted and unencrypted inbound Web traffic.
- Understanding how much work your staff will undertake is a critical decision factor in whether you employ a WAF and how. Avoiding false alerts ("false positives"), in particular, requires specific attention.
- Enterprises tend to focus their WAF efforts on compliance or protecting public-facing custom Web applications, but often neglect equally important internal applications.

Recommendations

Security leaders should:

- Strive for more than PCI compliance. Assess the need for Web application firewalls, based on the business impact of each Web application — public-facing, partner-facing or internal — rather than protecting public-facing Web applications only.
- Evaluate and deploy WAF technology, in combination with alternative security safeguards, such as application security testing and secure coding practices.
- Evaluate which deployment use cases are acceptable for your organization, and understand the specific challenges for each.
- Invest enough time in training security staff, conducting initial configuration tuning during the learning period and performing integration with other network security technologies. Then, continuously monitor and update the WAF configuration to gain the benefits from the technology.

What You Need to Know

WAFs are deployed on or in front of Web servers, and include protection techniques dedicated to the granular protection of specific Web applications. WAFs combine negative (protecting against known attacks) and positive (enforcing legitimate traffic only) security models to detect and protect against Web attacks and reduce the risk of false positives.

Security professionals sometimes confuse WAFs with NGFWs, or estimate that WAFs do not bring enough value to justify the cost when compared with IPSs. Organizations already equipped with best-of-breed firewalls and IPSs might view WAFs as an exponential investment for incremental benefits. However, IPS protections against Web vulnerabilities are too general; often limited to known vulnerabilities from off-the-shelf third-party libraries and frameworks. These protections are also mostly disabled by default. Corporate websites and Web applications carrying business-critical operations, such as for payroll, e-banking transactions and e-commerce orders, often include a combination of custom code, with self-inflicted vulnerabilities and third-party components. CIOs can't decide to leave critical Web servers untouched for fear of false alerts or service interruptions, because the complex Web languages (HTML5, JavaScript) give attackers attractive targets.

Security leaders should consider investing in WAFs, application security testing and secure coding tools if their organization owns public websites, makes internal Web applications available to partners and clients, or has business-critical internal Web applications. Organizations that

receive the greatest benefits from WAFs will go beyond compliance. They will spend enough time to select the right WAF deployment scenario, train operational staff, tune the different protections and monitor the infrastructure closely.

Analysis

In the early 2000s, most enterprises were not using WAFs to protect their Web servers and applications. Firewalls were the best practice, and intrusion detection and prevention were still maturing. The relatively low complexity of the Web applications was not a sufficient driver to justify an additional investment, and attackers were not yet backed by well-funded organizations.

Since then, Web applications have become more complex, relying on languages and scripts such as HTML5, Java, JavaScript, and PHP for rich interface application (RIA),extensive frameworks and complex third-party libraries. False positives and performance hits arising from protections that relied on traffic-pattern matching became a real issue. IPS vendors elected to disable most of the Web application protection signatures by default to mitigate these issues. Type A organizations realized the need for a new approach to Web application security, and have added WAFs to their security portfolios.

In 2008, the PCI Security Standards Council (PCI SSC) released the PCI Data Security Standard (PCI DSS) 1.2 with an updated requirement 6.6, which allowed WAFs as a viable alternative to Web application vulnerability assessments.[1] The PCI requirement has given additional momentum to the WAF market, helping it expand beyond niche use cases, especially in financial and banking organizations.

Unfortunately, many enterprises and WAF vendors use the low PCI compliance standard as the goal and do not seek more than a successful audit. Good Web application security requires more than a checkbox approach. Most WAFs can provide the PCI check mark but, as history often reminds us, compliance is not automatically equivalent with good security. Competitive evaluations for WAF technologies are still complicated and require a lengthy proof of concept, because similar feature names mask significant discrepancies in security depth. Once in production, WAFs continue to demand close monitoring to deliver high value.

This research covers the major features of WAF technology, explains the deployment options and provides selection guidelines. It will help security leaders responsible for Web application security projects to better understand the benefits and challenges of WAF implementation.

Technology Description

Web application firewalls protect Web servers and hosted Web applications against attacks at the application layer and nonvolumetric attacks at the network layer. It can be deployed as an endpoint agent on the Web server, a software or hardware network appliance, a software module hosted on an application delivery controller (ADC; see "Magic Quadrant for Application Delivery Controllers"), a virtual appliance or a cloud service (see Figure 1). Most of the time, WAFs are in-line, acting as a reverse proxy, but other deployments are available, such as transparent proxy, network bridge or out-of-band.

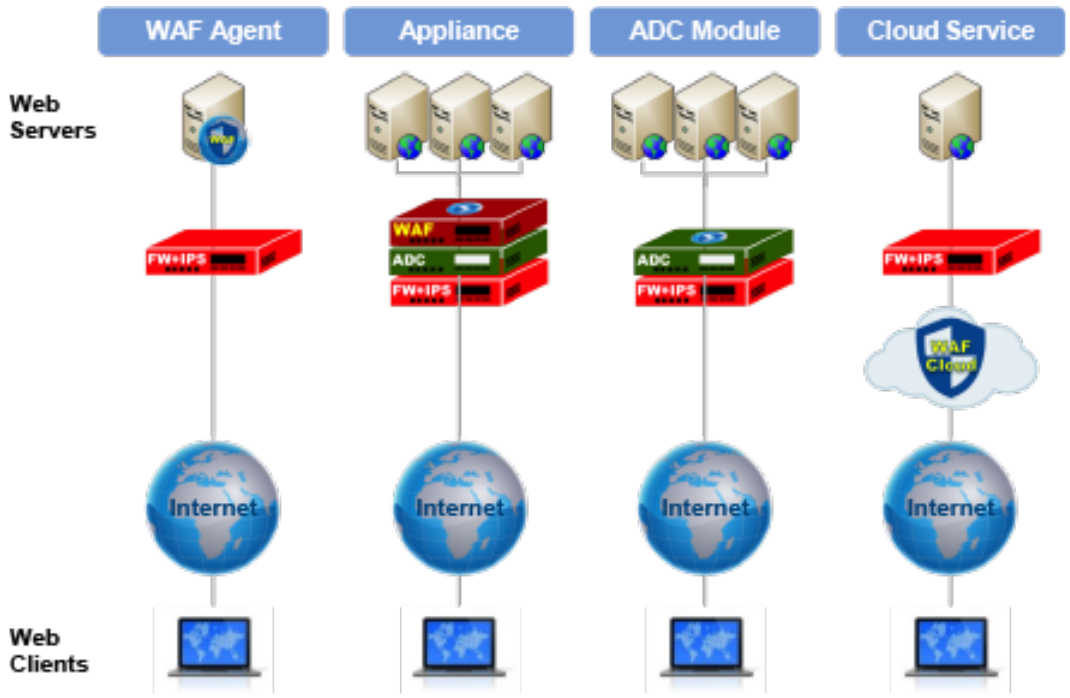
Web Attacks Command More Than Signatures

Threats against Web applications are well-documented. The Open Web Application Security Project (OWASP) Top Ten, CWE/SANS Top 25 Most Dangerous Software Errors and Web Application Security Consortium (WASC) Threat Classification v2.0 and Cross Reference View can help raise awareness of the threat landscape, providing elements to justify the need for technology dedicated to Web application security. However, security staff often fail to explain how WAFs can provide deeper, more-granular Web application safeguards than NGFWs and IPSs. Figure 2 highlights feature differences between NGFWs, IPSs and WAFs when it comes to Web application security.

Firewalls and IPSs provide signatures, mostly against SQL injection (SQLi) or cross-site scripting (XSS), but do not include more advanced features that WAF technologies can offer, such as:

- **Contextualized Web traffic inspection:** WAFs embed dedicated inspection engines for Web protocols and languages, to perform traffic decoding and normalization before applying in-context security inspection. This improves the effectiveness of Web attack and Web vulnerabilities signatures.

Figure 1 | Web Application Firewall Deployment Options for On-Premises Web Applications



Source: Gartner (February 2014)

Figure 2 | Main Differences Between WAF, IPS and NGFW

	Web Application Firewall	Intrusion Prevention System	Next-Generation Firewall
Multiprotocol Security	○	●	●
IP Reputation	◑	◑	◑
Web Attack Signatures	●	◑	○
Web Vulnerabilities Signatures	●	◑	◑
Automatic Policy Learning	●	○	○
URL, Parameter, Cookie, and Form Protection	●	○	○
Leverage Vulnerability Scan Results	●	◑	○

● = good to very good ◑ = average or fair ○ = below average

IP = Internet Protocol
Source: Gartner (February 2014)

- **Automatic policy learning:** The WAF security engine listens to HTTP requests/answers for configured Web domains, creates a map of URLs and different parameters, then suggests appropriate whitelisting enforcements (often called positive security models).
- **"Virtual patching":** The name is an overstatement. The WAF can leverage data from dynamic application security testing (DAST) tools to suggest or automatically enable additional controls/signatures to protect against the detected threats. The level of value provided highly depends on the quality of the vulnerability assessment tool.
- **Anti-automation:** This distinguishes real humans from automated clients that would interact with a Web application.
- **Business logic defense:** WAFs monitor user sessions to detect attacks that exploit business transactions in order to perform malicious activities that disrupt a normal business practice.
- **Anti-DDoS:** WAFs might include protection against application-targeted distributed denial of service (DDoS), but can't mitigate volumetric attacks. Vendors with a cloud offer often try to upsell their anti-DDoS solutions to their clients using WAFs.

These features are not the only differences between WAFs and other network security technologies. IPS appliances can operate out-of-band, on a copy of the traffic — or in-line, in bridge mode. While a few WAF technologies support these two deployment modes, most of them use the more intrusive reverse or transparent proxy modes. Acting as a proxy allows additional operations:

- **Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) decryption/offloading:** Reverse or transparent proxy modes allow decryption of TLS traffic when using cipher suites that enable forward secrecy[2] (Ephemeral Diffie-Hellman [DHE] and Elliptic Curve Diffie-Hellman [ECDH]). For other ciphers, WAFs might offer the ability to decrypt a copy of the encrypted traffic, when deployed in in-line bridge mode, or out-of-band.
- **Web content modification:** WAFs modify the responses sent by Web applications with techniques such as cookie signing, URL encryption, custom error page, and code injection in Web pages (for example, to prevent cross-site request forgery [CSRF]).
- **Authentication services:** WAFs can provide single sign-on for existing Web applications, or act as an authentication broker for legacy applications that don't have any authentication in place.

The ability for WAFs to decrypt SSL traffic makes a big difference when compared to NGWFs and IPSs. In 2013, Gartner conducted an industry survey of network security vendors and enterprises to find out how organizations are tackling the challenge of traffic decryption. The survey revealed that less than 20% of organizations with a firewall, an IPS or a unified threat management (UTM) appliance can decrypt inbound or outbound SSL traffic. However, more than 90% of organizations with a public website and a WAF can decrypt inbound Web traffic.

WAF technology might provide many other features, including ad hoc reports for PCI audit, multiprotocol inspections to cover other services provided by Web applications (such as FTP), Web service security, or remote user/host fingerprinting.

Technology Definition

A Web application firewall is a shielding safeguard intended to protect applications accessed via HTTP and HTTPS against exploitation. WAFs focus primarily on Web server protection at Layer 7 — the application layer — which includes classes of "self-inflicted" vulnerabilities in configured commercial applications, or in custom-developed code that makes Web applications subject to attacks. WAFs may also include safeguards against attacks at other layers.

Uses

Enterprises primarily use WAFs to protect public Web applications, as well as custom and internal applications such as payroll, Web mail or extranet. On rare occasions, organizations also use WAFs to protect their on-premises internal applications, such as intranet, since these applications are some of the easiest targets for attackers looking for a lateral move after an initial infection. WAF projects can be driven by compliance issues or initiated to improve the security of business-critical Web applications. At times, organizations leverage other

infrastructure projects to include WAFs in an ADC deployment or within a DDoS mitigation project.

Benefits and Risks

WAF technology leverages the knowledge gained on Web applications via careful monitoring of the applications' behavior to implement tightened security controls. When correctly implemented and tuned, WAFs are the technology of choice to enhance the security of existing Web applications. However, when organizations don't invest enough energy in their WAF deployment, they often face disappointing results.

Risks:

- False positives are the most important risk when deploying WAFs. Fear of false positives affects many WAF implementations and can lead to the displacement of the technology.
- Automatic policy learning can fail in various ways. If using a WAF as a permanent monitoring tool is not the objective, this might be an important issue. Organizations with fast-changing Web applications sometimes never progress beyond the learning period, due to a fear of false positives. Security leaders should also anticipate business-specific use cases, like B2B commerce with a peak period at the end of every quarter, or e-commerce sites with annual events such as the holiday season at the end of the year.
- WAF inner vulnerabilities are more critical than for other network security technologies. When acting in reverse or transparent proxy mode, the WAF itself might be a target for attackers.
- WAFs don't protect against volumetric DDoS attacks, which can bring down public websites and Web applications allowing remote access.

Technology Alternatives

When compliance dictates the WAF implementation project, application security testing (AST) coupled with software development best practices often compete with the WAF budget.

Organizations should put effort into secure development practices through development staff training and static code analysis and scanning, and they should consider the use of specific sanitization libraries (see the OWASP Developer Guide). However, Web applications rely heavily on third-party modules or libraries, so the detection of vulnerabilities can fall out of the direct control of Web application development teams. Upgrading these components might not be possible in a timely manner, and network-based compensatory controls might remain necessary. Using penetration testing applications can complement a secure development approach to provide a better assessment of the risks for Web applications.

NGFWs and IPSs include signature sets for Web application protection. Enterprises might see them as a price-attractive solution compared with a dedicated WAF. As discussed earlier in the document, these technologies only offer a subset of the many protections techniques available with a WAF. Moreover, Web security signatures are disabled in most default configurations, which means the workload is transferred to the network security staff. Fine-tuning the configuration per Web domain might also be difficult, with technologies not optimized to be sufficiently granular.

Open-source, free Web application firewalls like the ubiquitous ModSecurity or the more recent IronBee often compete against commercial offers. Even when a commercial set of signatures is available, organizations should carefully assess what the true gains will be, since these solutions are likely to require much more configuration work and rely on signatures, which is the technology most prone to false alerts.

Other vendors, such as Shape Security or Juniper Networks, with its WebApp Secure offering, focus on a few innovative techniques to protect Web applications. On-server security applications (such as runtime application self-protection [RASP]) are also available.

Selection Guidelines

Organizations willing to perform a competitive assessment of WAF vendors might face unexpected difficulties. PCI compliance and the availability of various ad hoc threat lists shape many RFPs. Too often, the comparison shrinks to a list of features, which lacks the necessary depth to uncover true differences between WAF vendors.

The WAF market landscape includes many different categories of vendors: large and small WAF pure players, more general network security vendors, ADC vendors, and cloud service providers. A number of the vendors are also relative newcomers to the

WAF market, and are in the middle of an ambitious road map for Web application security. Organizations should understand the characteristics of each vendor to determine whether the vendor meets the organization's needs.

WAF Deployment Scenario Drives the Selection Process

Enterprises should first evaluate which deployments options are acceptable for them. Each deployment scenario brings its own challenges (see Table 1), and many WAF vendors provide only the reverse proxy mode.

In large-scale deployments in which organization use ADCs, the integration of WAF features will benefit from available performance optimization features and shared traffic processing efforts.

Once the deployment scenario is chosen, security leaders should take special care of high-availability requirements, including cluster upgrade procedures and their impact on the production environment.

Enterprises Need to Compare WAFs Beyond Datasheet Check Marks

Differences between WAF technologies regarding price and performance may be easily recognized from the start, but discovering discrepancies in protection techniques requires further investigation. Because

Table 1. WAF Selection Questions for Different Deployment Use Cases

Use Case	Major Challenges	Subsequent Questions
Internet-Hosted (Cloud)	• Need for SSL decryption (secret key management) • Protection of internal Web applications • Incident response • Opt out	• How do the organization's compliance requirements affect its ability to delegate SSL decryption? • How will the organization handle incidents and false alerts (monitoring and response)? • What is an acceptable SLA for each level of incident? • How long does it take to opt out from the WAF provider?
Reverse or Transparent Proxy	• Performance • Tighter dependency with Web application due to "man in the middle" approach	• How can the WAF scale up and scale horizontally (cluster)? • How does the WAF integrate or partner with load balancers/ ADCs? • What does the application team manage? What belongs to the security team?
In-line Bridge Mode	• SSL/TLS decryption with perfect forward secrecy • Limited ability to modify content	• What are the compensatory controls your organization can deploy to replace the features that require content modification? • Do (or will) the Web applications implement Diffie-Hellman cipher suites (forward secrecy)?
Out-of-band	• Restricted number of WAF vendors • Limited ability to block, and no ability at all to modify content • SSL/TLS decryption with perfect forward secrecy	• What are the acceptable compromises to keep this deployment scenario? What wouldn't be acceptable? • How will the organization handle incidents and false alerts (monitoring and response)? • Do (or will) the Web applications implement Diffie-Hellman cipher suites (forward secrecy)?

Source: Gartner (February 2014)

these differences exist (see Table 2 for examples), security leaders should not rely on vendor claims, but should use the proof of concept and request feedback from their peers to verify the efficiency of the different techniques in their own environment.

During WAF competitive assessment, security leaders should specifically question smaller WAF vendors and newcomers to the market about their reputation databases and their attack signatures databases. Be wary about miraculous generic approaches, especially for protections against XSS and SQLi. Even the most basic protections are tested against known tools like Metasploit, so it can be used as an exclusion criterion, but should not be considered as sufficient. In 2013, 650 XSS attacks and 150 SQLis have been added to the Common Vulnerabilities and Exposures (CVE) database.[3] Selecting a few known recent attacks and asking vendors about them will give security leaders a better sense of a vendor's coverage.

Organizations should also understand that some attacks, such as CSRF, are hard to catch, and that no turnkey preventive solution can guarantee a perfect protection.

Web Application Security Is the "Heavenly Realm" for Evasion Techniques

The complexity of programming languages used in Web applications, and the extensive use of third-party source code and third-party byte/binary code in the form of libraries or frameworks, create perfect conditions for evasion techniques. A single vulnerability can be triggered in various ways, an SQLi can be distributed over several URL or form parameters, or the same string can be encoded in alternate ways. In addition, browsers might interpret the same content in a different way.[4]

Table 2. Analyzing Depth of WAF Protection

Threat	Minimal Protection	More-Advanced Techniques
Cross-Site Scripting (XSS) SQL Injection (SQLi)	• Pattern-matching signatures aimed at catching keywords	• Analyzing requests and responses • Multiple pass for traffic normalization covering various evasion techniques • Aggregated and contextual scoring to reduce false positives • Supplementary ad hoc signatures for known attacks • Enforcement using whitelisting rules
Automatic Policy Learning	• None (manual import of site map) *or* • One-time period without automatic ending	• Behavioral analysis automatically disables signatures that would trigger false positives • Automatic policy update when application changes • Predefined templates for well-known applications (Microsoft SharePoint, Microsoft Outlook Web Access, etc.)
"Virtual Patching"	• None *or* • Manual import of vulnerability scan result *and/or* • Limited number of supported scanners	• Automatic enforcement for critical vulnerability • Ability to launch a second test to confirm that a vulnerability is patched • Impact assessment of "virtual patch" deployment to help with the administrator's decision

Source: Gartner (February 2014)

Security leaders should request from WAF vendors additional elements regarding how their technology can prevent known evasion techniques and anticipate upcoming new variants.[5] Evaluation should only take into account specific examples of real attacks and discard marketing statements that are not backed up with evidence.

As a start, the WASC's Web Application Firewall Criteria (WAFEC), despite their publication in 2006, remain a good independent template to cover the basics of a WAF selection RFP, even if organizations must adapt each section to their specific needs.

Price Performance

WAF pricing models might vary based on the vendors and their deployment use cases. While most vendors offer the traditional initial purchase coupled with maintenance and subscriptions bundles, a few WAF vendors add additional limits, such as the number of Web applications, server IP addresses, or the CPU core for software appliances. Additional limits based on performance metrics, such as the number of transactions per second, might also apply. Cloud providers use subscription fees (monthly or yearly), occasionally coupled with performance-related restriction (page views).

Gartner recommends that clients ask WAF vendors for simple pricing models and require proposals with total cost of ownership for multiple years, including all the recurring subscriptions. Performance measurement can't be reliably assessed from vendor's collaterals, and should be confirmed during a proof of concept. Additional costs for SSL acceleration might significantly impact the total cost. Moreover, Gartner observes that many WAF deployments face unexpected short life cycles due to a lack of anticipation of growing application traffic. Organization should provision for growing Web and encrypted traffic based on trends observed in the past and knowledge of upcoming changes in their application offers.

Technology Providers

Sample WAF Vendors:

- A10 Networks
- AdNovum
- Akamai Technologies
- Anchiva
- Barracuda Networks
- Bee Ware
- BugSec
- Citrix
- CloudFlare
- DBAPPSecurity
- DenyAll
- Ergon Informatik
- F5 Networks
- Fortinet
- Igaware
- Imperva
- Nsfocus
- Penta Security
- Positive Technologies
- Qualys
- Radware
- Riverbed
- Sangfor
- Sucuri Security
- Trustwave
- United Security Providers
- Venustech

Sample Open-Source Projects:

- ModSecurity
- IronBee

Evidence

[1]"Payment Card Industry (PCI) Data Security Standard — Requirements and Security Assessment Procedures Version 1.2," October 2008; and "PCI Data Security Standards Council — Information Supplement: Application Reviews and Web Application Firewalls Clarified," October 2008.

[2]"SSL/TLS & Perfect Forward Secrecy," by Vincent Bernat, 2011.

[3]"Common Vulnerabilities and Exposures Details."

[4]"The InnerHTML Apocalypse: How mXSS Attacks Change Everything We Believed to Know So Far," by Mario Heiderich, Muenster University of Applied Sciences, 2013.

[5]"Protocol-Level Evasion of Web Application Firewalls," by Ivan Risti, 25 July 2012.

Gartner RAS Core Research Note G00258206, Jeremy D'Hoinne, Adam Hils, 28 February 2014
07 January 2014

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. We are among the world's most advanced specialist researchers, renowned security experts and highly-skilled programmers.

With one of the largest and most dynamic research facilities in the world, Positive Technologies carries out research, penetration testing and threat and vulnerability analysis on dozens of large-scale networks each year. As a result we have developed a unique understanding of how security should work, across a wide range of geographies and systems. We earned our reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, anywhere.

Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring your company's compliance with regulatory requirements and corporate standards; and blocking real-time attacks. Positive Technologies will give you complete confidence in the security of your network, its associated policies and its related applications.

Hands-on experience, underscored by a decade of service to clients worldwide, has enabled Positive Technologies to develop a thorough knowledge and understanding of vulnerability and compliance management that is unmatched. Our commitment to clients and track record of research excellence has earned Positive Technologies distinction as one of the fastest growing Security and Vulnerability Management firms in in the world.

To learn more about Positive Technologies please visit www.ptsecurity.com

A SMARTER APPROACH TO APPLICATION SECURITY is published by Positive Technologies. Editorial content supplied by Positive Technologies is independent of Gartner analysis. All Gartner research is used with Gartner's permission, and was originally published as part of Gartner's syndicated research service available to all entitled Gartner clients. © 2014 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner's endorsement of Positive Technologies's products and/or strategies. Reproduction or distribution of this publication in any form without Gartner's prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.