# Be a Web App Security Superhero

Faced with threats like never before, security pros must consider WAFs, RASP and other new security tools to hone their crime-fighting superpowers.

# Hone Your Superpowers for Web App Security

**Superheroes change by** generation: Superman, Batman, Spider-Man, the Mighty Morphin Power Rangers—even SpongeBob Squarepants. Precisely who kept you glued week after week to the television screen likely depends on what year you first figured out the remote. But the battle between good and evil, the fight to protect society's valuable assets against evildoers—that never changes.

InfoSec pros are the enterprise network superheroes, who use their very special powers to ward off the bad guys attacking the network. This three-part guide focuses on the latest security tools and methods designed specifically to protect the Web applications on that network.

First, Brad Causey presents a thorough overview of the Web application firewall. WAFs, developed originally to specifically respond to the threats against applications and related infrastructure, have gained even more powers recently. They're particularly effective, as Causey elaborates in our second chapter, when teamed up with application testing.

No discussion of ways to secure apps would be complete without a review of the latest trend in app security, known as runtime application self-protection. So in our closing chapter Nicole Laskowski details how RASP can deliver breadth to your security posture, but also notes why RASP alone isn't the answer.

Read on to learn the latest in how to secure Web apps on your enterprise network. ■

Brenda L. Horrigan, Ph.D.
*Associate Managing Editor*
*SearchSecurity*

# Mighty Morphing Firewalls Tackle Threats to Your Network

FIREWALLS HAVE SIGNIFICANTLY improved the overall security posture of organizations since they first came on the scene back in the late 1980s. Like everything else, though, firewalls have evolved. They've morphed to adapt to new technologies and, more importantly, new threats.

Enter Web application firewalls, or WAFs.

Developed in the early 1990s, WAFs were a new species of firewall initially created to respond to threats beyond the scope of traditional firewalls. These threats were dangerous because they utilized authorized protocols (such as HTTP), but attacked the application or underlying infrastructure over that protocol. This was especially dangerous because hackers could attack over trusted protocols to directly compromise systems and steal information, effectively bypassing traditional firewalls.

Modern WAFs have evolved into a number of different implementations, each carrying its own cost/benefit matrix.

## WEB APPLICATION FIREWALL BASICS: THREE DEPLOYMENT OPTIONS

WAFs are available in three rather broad categories: network-based, application-based and cloud-hosted.

Network-based WAFs are the traditional implementation of the technology. It offers several benefits and drawbacks. The largest benefit is that network-based WAFs are usually hardware-based and, being local, it reduces

> Like everything else, firewalls have evolved. They've morphed to adapt to new technologies and, more importantly, new threats.

latency and negative performance impacts. The largest drawback is that this type of WAF product tends to be more expensive to both purchase and implement.

Application-based WAFs are generally installed closest to the application, such as on the hosting platform, and often times are fully integrated into the application code itself. The benefits of this type of WAF implementation are increased performance and customization options. As an example, since ModSecurity (an open source WAF) can be installed as a module in Apache, an application can take full advantage of the features while allowing the overhead to be handled by the server locally. The cost of deploying an application-based WAF is typically low as well, but the flexibility and scalability can leave something to be desired for larger organizations.

Cloud-hosted WAFs, meanwhile, offer a low-cost/low-effort application firewall implementation opportunity for organizations that want a turnkey product. These are easy to deploy, as they often require only a simple DNS change to redirect application traffic, and are available on a subscription basis. While customization and performance limitations are usually drawbacks of cloud-based WAF products, they are often a viable stop-gap product that can be deployed rapidly.

## USING WAFs TO HELP SECURE APPLICATIONS AND NETWORKS

The real challenge of providing Web services in any form is securing them against attacks. That's why any organization with technology exposed to the Internet can benefit from having a WAF. This, of course, describes most businesses today.

Even those with something as simple as a website hosted on the Internet are at risk of exposure. Include with that any services offered to customers over the Internet, or any intranet interfaces between business partners, and the list of reasons to deploy a WAF starts to grow.

Because of the nature of Web security and how it constantly evolves, it is difficult to integrate comprehensive security into the application and keep it up to date. Having a WAF helps here in two ways: It protects against known threats (just like antivirus software) and it protects against unknown threats.

SQL injections are examples of known threats that are easily detected by a WAF. They're usually stopped by a combination of input validation and database-level protections by WAFs.

While it's impossible to know what the threats of tomorrow may be, if a threat utilizes an overflowing form field as a means of attack, a WAF can still stop it—even if the application is not coded to handle it.

## WHO BENEFITS MOST FROM WEB APPLICATION FIREWALLS?

While organizations of all sizes can make use of a WAF, the market section that will benefit most from the technology is that which provide products over the Internet. So the likes of Web hosts, online bankers, social media platform providers and even mobile application developers (the latter leveraging cloud-based WAFs, for instance) can take advantage of the centralized control and update capabilities of a WAF in order to increase the security posture of applications.

## MANAGING AND SUPPORTING WEB APPLICATION FIREWALLS

WAF management and support structure depends largely on how it's implemented.

For network-based WAFs, the IT security or network team will often manage its configuration for the organization. Management of these is usually offered as a managed service by the vendor as well, making administration fairly straightforward and simple. And, because WAFs use a central set of signatures and configuration options, dozens of applications can be protected with much less effort and expense. Additionally, most major network-based WAF vendors allow replication of

It's impossible to know what the threats of tomorrow may be, but if it uses an overflowing form field as a means of attack, a WAF can stop it.

rules and settings across multiple appliances, thereby making large scale deployment and configuration possible.

Application-based WAF scan be a challenge to manage because they live locally but are usually integrated into the application. In other words, application-based WAFs require local libraries, compatible environments (such as Java or .NET) and use local server resources to run effectively. They are also entirely software-based, so a combination of the server-management and security teams will likely need to be involved with installation and management.

Cloud-based WAFs are usually managed by the service provider with a configuration interface made available to the customer. The interface will usually allow the security or application team of the customer to customize the settings of the firewall. These settings can include how the WAF will respond to certain threats, such as SQL injection, or even a distributed denial-of-service attack. They also include notification options and the ability to turn off certain rule sets.

No matter who manages a WAF, an organization's application or development team must also be involved in its administration. Why? Because an incorrectly configured WAF can have a negative impact on the availability and performance of the application it's tasked with protecting.

**By bringing in consultants, or professional services, a business can avoid training IT staff and speed up the implementation of a newly installed WAF.**

Some management training of IT staff will be required no matter which type of WAF is implemented. In most cases, the more in-depth a configuration management role a company wishes to play, the more training will be required.

As an alternative, professional services can eliminate this effort, for a fee. By bringing in consultants, or professional services, a business can avoid having to train existing IT staff, speed up the implementation of a newly installed WAF, or pay them to manage an existing WAF long term.

HOME

EDITOR'S NOTE

MIGHTY MORPHING FIREWALLS TACKLE THREATS TO YOUR NETWORK

WAFs AND APP TESTING, SECURITY'S DYNAMIC DUO

IT'S RASP TO THE RESCUE—OR IS IT?

## THE HARD AND SOFT COSTS OF WEB APPLICATION FIREWALL DEPLOYMENT

The hard cost of a WAF varies widely from "free" to millions of dollars. Hard costs are associated with the cost of the physical components required to implement the technology. There are open source WAF implementations that can be downloaded and installed for no hard cost, for example, but those often have substantial soft costs, involving development time, staff training and/or supporting efforts.

> **The hard cost of a WAF varies widely from "free" to millions of dollars.**

In addition, the type of WAF chosen affects the hard costs involved for deployment and support. And, keep in mind, any time the behavior of an application is significantly altered, there will be a proportionate jump of soft costs in time and effort.

Cloud-based WAFs are significantly cheaper to deploy and support than network-based (hardware) WAF products. Application-based WAFs fall somewhere between the two, and would be more suited for a small application footprint.

## WHAT A WEB APPLICATION FIREWALL IS *NOT*

A WAF is not a replacement for proper application security, such as input filtering and user authentication/authorization. It is intended as one component in a layered approach to a secure Web application.

It is also not a set-and-forget technology. As an application changes and the threats evolve, care must be taken to properly maintain rules and configuration options.

It is also important to differentiate a WAF from a next-generation firewall, or NGFW. A WAF is intended to inspect the application traffic on a narrow protocol scope and focus only on that traffic. A NGFW is a comprehensive product to replace or augment existing network firewalls.

NGFWs may sometimes include WAF components, but are intended to operate on a much larger scope (and cost) within the organization.

*—Brad Causey*

# WAFs and App Testing, Security's Dynamic Duo

As Web-based application deployments have grown exponentially during the past decade, so have security concerns with all points involved in their delivery of those applications. In this chapter, we will discuss the roles of application security testing and Web application firewalls (WAFs). You will learn why each has its place, and how they can combine and complement each other to strengthen your overall application security posture.

From the Web browser to the SSL/TLS protocols to the Web application itself, the industry has been fighting to secure the mechanisms through which the application layer can be exploited. Enterprises won't be able to prevent every zero-day or creative exploit—nor should they try. By focusing on what we can do, as application owners and developers, we can secure our applications from attackers and protect our users from undue risk.

## APPLICATION SECURITY TESTING

There are a couple of places to start, but two stand out. The first, application security testing, is certainly the most effective way to detect, fix and resolve security issues within applications.

As part of a secure software development lifecycle (SDLC), application testing can detect security issues early in the cycle, or later in acceptance testing, depending on the method you use. Static code analysis produces a lot of false positives, but provides the most

**From the Web browser to SSL/TLS protocols to the application itself, the industry must fight to secure the application layer against attack.**

comprehensive view—earlier than other types of testing. Dynamic testing results in more concrete findings, but can be time consuming and its findings are not always comprehensive. Ideally, a combination of both static code analysis and dynamic testing, discussed further below, balance their advantages and will significantly augment the security posture of your applications.

The trouble, though, is that in-depth application testing isn't always possible, due to time constraints, license agreements or code availability (among various other reasons). Because of this, WAFs offer another viable option to app security.

### WEB APP FIREWALLS

WAFs can be integrated or stood up in front of your application to quickly reduce your applications' exposure to attack. This option, though, isn't without compromise.

WAFs work by standing between the user and the application, and that will cause performance issues, and also require time and expertise to deploy. Bear in mind, though, that a WAF is also not a perfect solution. Most WAFs will do a stellar job in catching obvious attacks, such as SQL injection or cross-site scripting. Issues such as business-logic bypasses or functional issues will have to be addressed through code or custom rules in your WAF; don't forget this important step, as they can be just as harmful to application security as a traditional security "bug" may be.

The great thing, though, about WAFs is that they are relatively quick to install and can work to shore up your applications' security, even if you don't have the ability, time or permission to perform static or dynamic analysis.

### THE SECURITY ONE-TWO PUNCH

A third, even better, option is a combination of software security best practices during the design and development of the applications, as well as application security controls after the Web app is implemented. Why not have both?

Integrate security into application design, coding and testing phases; many organizations have created blueprints for establishing a comprehensive, effective SDLC. Inevitably security flaws will be discovered in applications after they are in production environments, some of which will be easier to patch than others; that's where the WAF comes into play, buying your organization some time to sort out any security issues that are discovered after the development phase by preventing exploitation until they can be permanently resolved.

These two methods of minimizing application risk actually go quite well together. In many cases, companies will roll the security patch or fix in the next release, while defining specific rules within the WAF to address those issues. This is especially useful for security issues that require major effort to resolve.

*—Brad Causey*

# It's RASP to the Rescue—Or Is It?

In the application economy, a perimeter defense is no longer a good offense. With the proliferation of mobile devices and cloud-based technologies, perimeters are all but disappearing, according to Joseph Feiman, an analyst with Gartner Inc. "The more we move from place to place with our mobile devices, the less reliable perimeter-based technology becomes," he said.

Firewalls and intrusion prevention systems, which enterprises spent an estimated $9.1 billion on last year, still serve a vital purpose. But, given the enterprise infrastructure's growing sprawl, CIOs should be thinking about security breadth as well as security depth and how to scale their strategies down to the applications themselves, even building in a strikingly human feature: self-awareness.

A new tool for the application security toolbox known as runtime application self-protection (RASP) could help CIOs get there, but, according to one expert, it's no silver bullet.

## GUARDING THE APPLICATION

The security measures many CIOs have in place don't do much to safeguard actual applications, according to Feiman. Network firewalls, identity access management, intrusion detection or endpoint protection provide security at different levels, but none of them can see beyond the application layer. "Can you imagine a person who walks out of the house and into the city always surrounded by bodyguards because

**CIOs should be thinking about security breadth as well as security depth and how to scale their strategies down to the applications themselves.**

he has no muscles and no skills," Feiman said. "That is a direct analogy with the application." Strip away features like perimeter firewalls, and the application is basically defenseless.

Defenseless applications leave enterprises vulnerable to external—and internal—threats. "High-profile security breaches illustrate the growing determination and sophistication of attackers," said Johann Schleier-Smith, CTO at if(we), a social and mobile technology company based in San Francisco. "They have also forced the industry to confront the limitations of traditional security measures."

Application security testing tools help detect flaws and weaknesses, but the tools aren't comprehensive, Feiman said during a Gartner Security and Risk Management Summit last summer. Static application security testing, for example, analyzes source, binary or byte code to uncover bugs but only before the application is operational. Dynamic application security testing, on the other hand, simulates attacks on the application while it's operational and analyzes the response but only for Web applications that use HTTP, according to Gary McGraw, CTO of the software security consulting firm Cigital Inc.

Even when taken together, these two technologies still can't see what happens inside the application while it's operational. And, according to Feiman's research report "Stop Protecting Your Apps; It's Time for Apps to Protect Themselves," published in September 2014, static and dynamic testing, whether accomplished with premises-based tools or purchased as a service, can be time-consuming and hard to scale as the enterprise app portfolio multiplies.

## IS RASP THE ANSWER?

RASP, which can be applied to Web and non-Web applications, doesn't affect the application design itself; instead, detection and protection features are added to the servers an application runs on. "Being a part of the virtual machine, RASP sees every instruction being executed, and it can see whether a set of instructions is an attack or not," he said. The technology works in two modes: It can be set to diagnostic mode to sound an alarm; or it can be set to self-protection mode to "stop an execution that would lead to a malicious exploit," Feiman said.

The technology is offered by a handful of vendors. Many, such as Waratek, founded in 2009, are new to the market, but CIOs will recognize at least one vendor getting into the RASP game: Hewlett-Packard. Currently, RASP technology is built for the two popular application servers: Java virtual machine and .NET Common Language Runtime. Additional implementations are expected to be rolled out as the technology matures.

While Feiman pointed to the technology's "unmatched accuracy," he did note a couple of challenges: The technology is language dependent, which means the technology will have to be implemented separately for Java virtual machine versus .NET CLR. Because RASP sits on the application server, it uses CPUs. "Emerging RASP vendors report 2% to 3% of performance overhead, and some other evidence reports 10% or more," Feiman wrote in *Runtime Application Self-Protection: Technical Capabilities*, published in 2012.

## IS IT READY FOR PRIMETIME?

Not everyone is ready to endorse RASP. "I don't think it's ready for primetime," said Cigital's McGraw. RASP isn't a bad idea in principle, he said, "but in practice, it's only worked for one or two weak categories of bugs."

The statement was echoed by Schleier-Smith: "What remains to be seen is whether the value RASP brings beyond Web application firewalls and other established technologies offsets the potential additional complexity," he said.

CIOs may be better off creating an inventory of applications segmented by type—mobile, cloud-based, Web-facing. "And choose the [security] technology stack most appropriate for the types of applications found in their portfolio," McGraw said.

> **"What remains to be seen is whether the value RASP brings ... offsets the potential additional complexity."** — **JOHANN SCHLEIER-SMITH,** CTO, if(we)

Even Feiman stressed that CIOs need to find a use case for the technology and also consider how aggressive, in general, the organization is when adopting emerging technologies. For more conservative organizations, investing in RASP could still be two to five years out, he said.

To strengthen application security right now, McGraw urged CIOs to remember the power of static testing, which works on all kinds of software. And he suggested they investigate how thoroughly tools such as static and dynamic testing are being utilized by their staff. "The security people are not really testing people," he said, referring to software developers. "So when they first applied dynamic testing to security, nobody bothered to check how much of the code was actually tested. And the answer was: Not very much."

An even better strategy: Rather than place too much emphasis on RASP or other forms of security testing, application security should start with application design. "Half of software security issues are design problems and not silly little bugs," McGraw said.

—*Nicole Laskowski*

**BRAD CAUSEY,** *CEO of Zero Day Consulting, is an active member of the world security and forensics community, focused on Web Application security as it applies to global and enterprise arenas. He is president of the International Information Systems Forensics Association chapter in Alabama.*

**NICOLE LASKOWSKI** *is senior news writer for TechTarget's SearchCIO.com, where she covers analytics, business intelligence and data management.*

**STAY CONNECTED!**

Follow @SearchSecurity today

*Be a Web App Security Superhero*
is a SearchSecurity.com e-publication.

**TechTarget**
275 Grove Street, Newton, MA 02466
www.techtarget.com

**About TechTarget:** TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER ART: ISTOCK