

White Paper

Understanding Web Application Security  
Defending the Enterprise's New Porous Perimeter  
by Extending Security to the Edge



# Table of Contents

- EXECUTIVE SUMMARY ..... 1
- INTRODUCTION..... 1
  - The Escalating Risk of the Insecure Web..... 1
- THE CHALLENGES ..... 2
  - The Enterprise’s New Porous Perimeter ..... 2
- TRENDS IN WEB-BASED ATTACKS ..... 3
  - Cyber Crime Goes Pro ..... 3
  - Web Sites as Attack Vendors ..... 3
  - Automation and Armies ..... 3
  - Major Web Application Threats ..... 4
- EXISTING SECURITY APPROACHES..... 4
  - Secure Coding and Code Review Practices ..... 4
  - Centralized Web Application Firewalls ..... 5
- AKAMAI WAF: A DISTRIBUTED APPROACH TO WEB APPLICATION SECURITY ..... 5
  - How Akamai WAF Works ..... 6
  - Distributed WAF Architecture..... 6
- AKAMAI WAF BENEFITS ..... 7
  - The EdgePlatform Advantage..... 7
  - Optional Advantages ..... 8
  - Business Benefits ..... 8
- DEFENSE-IN-DEPTH WITH AKAMAI WAF ..... 9
- ABOUT AKAMAI SECURITY..... 10

## Executive Summary

As enterprises move more of their business transactions online, they face the challenge of defending a perimeter that grows increasingly porous. Proprietary data and business-critical operations are being exposed through Web interfaces that are accessible from anywhere in the world and highly vulnerable to the Internet's growing threat environment.

The network firewalls that once locked down the enterprise perimeter are ineffective against Web-based attacks that are quickly rising in frequency, scale, and severity. These Layer 7 attacks now account for between 60 and 80% of all reported security incidents.<sup>1</sup> By exploiting common Web application security flaws, the attacks are able to cause tremendous business disruption, particularly through the theft of sensitive enterprise information as well as customer and employee personal data.

This paper examines current trends in Web application security, assessing the present threat environment as well as limitations in existing approaches to protection. It then looks at how Akamai's new distributed Web Application Firewall solution overcomes these challenges, working as an integral part of a defense-in-depth security architecture to provide robust and scalable protection that is both practical and cost effective.

## Introduction

### The Escalating Risk of the Insecure Web

Cyberspace is sometimes called the silent battleground, as both hackers and hacked want to stay off the public radar screen. However, the harm being done to businesses' online presence is very real. Every industry is at risk: retail and financial sites are targeted for credit card and account data; enterprises are targeted for intellectual property and proprietary data; government organizations are targeted for political or ideological reasons; and popular Web sites—including social media, online gaming, and entertainment destinations—are targeted for their massive user base. Small businesses are not safe either, as many attacks are untargeted, with cyber criminals using automated methods to detect and infect vulnerable sites.

Application layer attacks in particular are one of the biggest threats enterprise IT faces today. These attacks are proliferating as criminals look to exploit the highly vulnerable and largely unprotected Web application layer that serves as the new enterprise perimeter—one that unfortunately gives inadequate protection to the business-critical data and operations within.

The damage being inflicted is serious. A recent Purdue University study involving more than 800 CIOs estimates that cyber crime cost businesses more than \$1 Trillion in 2008, through theft of data and intellectual property, as well as damage to customer trust and brand reputation. Repairing the fallout from data breaches is costly, as businesses can be subject to reporting and notification requirements as well as lawsuits and fines.

Regulatory compliance is another issue. The credit card industry, for example, has implemented specific regulatory requirements to ensure that merchants involved in online credit or debit card transactions secure their Web applications in order to safeguard customer account data.

Unfortunately, as enterprises attempt to harden their applications and secure their perimeters, they will face a number of challenges, including a complex and vulnerable application environment as well as increasingly sophisticated attacks that can render traditional, centralized security solutions ineffective.

## The Challenges

Over the last several years, many enterprises have migrated their business-critical transactions to the Web in order to take advantage of its broad reach and enormous efficiencies. But the Internet was never designed to be a secure or reliable platform; its early adopters never foresaw the central role it would come to play. As a result, Web applications now connect critical enterprise data to this very open, public, and inherently insecure platform, exposing businesses to increasing risks of disruption and compromise from a wide range of network threats.

### Web Applications: The Enterprise's New Porous Perimeter

As organizations have come to better understand and protect their network-layer security, cyber criminals have adapted, shifting their focus to the more complex and vulnerable application layer. Thus, as more and more mission-critical enterprise assets and operations are being exposed through Web interfaces, the applications themselves have become the new enterprise perimeter—one that is increasingly complex and porous.

Indeed, as a category, Web application vulnerabilities may represent the most serious—and under-protected—security flaws in enterprise IT infrastructure today. Security firm Sophos estimates, for example, that approximately 23,500 Web pages are infected every day, which means a new infection occurs every 3.6 seconds.<sup>2</sup>

There are a number of reasons for that Web applications are so susceptible to attack:

**Firewall Accessibility.** Traditionally, access to enterprise data and applications was limited to internal networks, and firewalls protected the enterprise's perimeter, locking down the boundary at Internet gateways. However, these network firewalls are generally configured to allow passage of HTTP and SSL traffic (ports 80 and 443), giving cyber criminals an open window through which to exploit application-layer vulnerabilities.

**Complex Architecture.** Most corporate Web sites began as simple, static brochure-ware, carrying a low security risk profile. Over time, functionality was added in an ad-hoc way, eventually turning the once-basic site into a rich application accessing critical backend systems, creating a serious security risk. The resulting site architecture is heterogeneous and complex, as new and legacy technologies are force-fit together, exposing numerous interfaces in the process. Consequently, it is difficult to understand, much less manage, the security risks and vulnerabilities present in the current Web site.

**Application Interactivity and Web 2.0.** The highly interactive nature of modern Web applications is also their biggest security weakness. If not properly validated, user inputs and user generated content in an application can be leveraged to access sensitive data or inject malicious code into a site. The visibility and manipulability of application code in browsers provides another window for easy exploitation; AJAX and other Rich Internet Applications that enable business logic to run on the client are particularly susceptible.

**Fast-Changing Technologies.** Today's high-function, feature-rich Web applications make use of many new and constantly evolving technologies, such as AJAX and Flash for interactive user interfaces, Web Services for system-to-system communications, and cloud computing solutions for cost-efficient and scalable infrastructure. In the race for functionality, many applications will be developed without a solid understanding of the security implications of these new technologies. In addition, Web developers must contend with the continual introduction and upgrade cycle of operating systems, application servers, browsers, and mobile clients. The complexity and rapid change in technology makes it all but impossible for organizations to keep their security solutions up to date.

**Rapid Development Cycles.** Finally, competitive pressures in the marketplace drive a focus on functionality and time-to-market, with security taking a back seat. Rapid application cycles and continual updates leave little time for proper code review and vulnerability testing, and thus allow for the continual introduction of new weaknesses.

## Trends in Web-based Attacks

These factors cited above have led to a highly complex and vulnerable environment for Web applications, and cyber criminals have been quick to capitalize. In fact, the common theme among recent trends is the rise in sophistication of these attackers and their arsenals, leading to the ability to inflict ever greater damages.

### Cyber Crime Goes Pro

Cyber crime used to be the realm of a lone hacker seeking fame, but it is now more often a professional money-making operation—one that reveals widespread influences from organized crime. Although cyber attacks can be motivated by political or ideological causes, financial gain is often the primary motive. Indeed, cyber-criminal activity is now easily monetized through a burgeoning black market, where hackers can buy or sell anything needed to ply their trade, including reconnaissance tools, customized malware, zombie networks, or massive lists of stolen IDs.

Credit card numbers and other personal financial account information are popular targets among cyber thieves, as card numbers can fetch anywhere from \$.10 to \$25 per account in the underground economy, and bank account credentials can sell for \$10 to \$1000 per account. Symantec estimates that the underground market for this stolen financial data is worth hundreds of millions of dollars, while the aggregate monetary value of the accounts themselves runs in the billions.<sup>3</sup>

In addition to targeting customer financial data, cyber criminals are also exploiting Web application security flaws to go after the enterprise's crown jewels. A recent McAfee security report notes that stolen intellectual property, driven by industrial espionage, is a fast growing target as hackers become increasingly sophisticated and aim for higher-value spoils.<sup>4</sup>

These lucrative financial rewards, combined with the low barriers to entry and relatively low risk involved, have propelled the sharp and continuing rise in cyber crime over recent years.

### Web Sites as Attack Vectors

Another major trend is the compromise of Web sites in order to infect the machines of site visitors—turning the site itself into an attack vector rather than a direct target. Although company data is not directly at risk in these types of attacks, brand and reputation are. Using techniques such as Cross Site Scripting or SQL Injection, attackers can take advantage of the trust, reputation, and popularity of a site in order to infect its visitors with malware.

According to Websense, in the first half of 2009, 61 of the top 100 most popular sites on the Web were found to have been compromised in this way—either hosting malicious content or containing a hidden redirect to a malicious site.<sup>5</sup> The malware possibilities are limitless; for example, they may install keystroke loggers to capture user password data, or rope the user's machine into part of a botnet that can be leveraged for other cyber attacks.

### Automation and Armies

To exacerbate matters, cyber criminals' arsenals are quickly growing in sophistication. Malware now incorporates advanced technologies to evade detection and removal, for example, and is increasingly written by professional hackers with R&D and testing departments who even support their releases with bug fixes and updates.<sup>6</sup>

Another key trend is the rise of automated attack tools, including the use of zombie armies or botnets, which magnify and multiply the possible scale of attacks. Unfortunately, an estimated 34 million computers in the United States may now be part of a botnet, a 50% increase over last year.<sup>7</sup> These armies of infected machines give attackers control over a massive number of computing resources, used to launch large-scale SQL injection attacks, distribute malware or spam, perpetrate password and credit card thefts, execute DDoS attacks, or protect malicious Web sites with fast flux hosting.

Botnets and malware are readily available through the black market, putting these sophisticated and powerful tools at anyone's disposal. This means it takes very little to carry out a wide-scale attack. In 2007, for example, a single disgruntled student was able to launch a crippling, month-long attack launched against the Estonian government and other commercial entities. Thus, enterprises must be prepared to deal with Web attacks on a massive scale.

## Major Web Application Threats

Unfortunately, while awareness of Layer 7 threats is growing, the vast majority of Web applications still remain largely unprotected. According to the Web Application Security Consortium, today more than 87% of Web applications carry a vulnerability classified as high risk or worse.<sup>8</sup> Moreover, nearly half of the tested Web applications contained critical or urgent vulnerabilities detectable with automated scanning.

We highlight some of the leading threats here.

**SQL Injection** – Numerous vulnerability-tracking databases cite SQL Injection as the most commonly exploited Web security flaw in 2008. One report notes that there were a few thousand SQL attacks per day at the start of 2008, but several hundred thousand per day by the year's end.<sup>9</sup>

SQL attacks exploit application vulnerabilities, such as user input fields that are not properly filtered, that allow SQL code to be maliciously inserted and executed in the database. Once the database is broken into, the possibilities are virtually limitless. Attackers can use the breach to steal or tamper with data, or install malware across multiple systems.

The massive Heartland and Hannaford Brothers data breach, which led to theft of 130 million credit and debit card numbers, was perpetrated by SQL injection. Extensive, botnet-driven SQL injection attacks have also been used to plant code on trusted

sites that redirects users to malicious sites where malware is planted on users' machines. Such an attack compromised over 70,000 Web sites in January 2008.<sup>10</sup>

**Cross Site Scripting (XSS)** – Cross Site Scripting is another common vulnerability, with one report estimating that 65% of websites are susceptible.<sup>11</sup> This vulnerability allows attackers to execute a malicious client-side script by injecting it into the URL of a trusted site. XSS enable theft of sensitive user data, including cookies or login information. It can also tamper with site content, leveraging social engineering techniques and the trusted site's reputation to trick users into downloading other malware.

**Distributed Denial-of-Service (DDoS)** – DDoS attacks are another fast-rising category, with both the number and size of attacks escalating quickly. According to one survey, denial of service attacks were second only to SQL injection as the most commonly reported Web vulnerability in the second half of 2008.<sup>12</sup> With the help of botnets, attackers are now able to execute denial of service attacks on a far greater scale than ever before, making them more difficult and costly to defend against. Moreover, application-layer DDoS attacks are harder to detect than network-layer DDoS attacks, as they use massive amounts of "normal" Web requests that may be difficult to distinguish from legitimate traffic.

## Existing Security Approaches

Traditional network firewalls and intrusion prevention systems provide insufficient security against these treacherous Web-based attacks. To augment these protections, there two primary approaches used today for securing the Web application layer. Each one has its practical limitations, as we will see, but a comprehensive security architecture is likely to leverage some techniques of each.

### Secure Coding and Code Review Practices

In theory, designing and building security directly into Web application code is an excellent approach to protecting sites. Best practices include strict code review at product design, development, testing, and deployment stages, using both automated and manual methods, including penetration testing and code vulnerability assessment tools.

In practice, however, companies lack the resources to carry out these time-intensive tasks consistently. It is also difficult for companies to maintain up-to-date, in-house expertise, as the technology and security landscapes evolve quickly.

Moreover, fixing flaws takes time—and expertise, particularly in today's complex, application environment. A recent WhiteHat study showed that companies took anywhere from one to four months, on average, to fix known Web site vulnerabilities that were rated either urgent, critical, or high risk. This number does not even account for vulnerabilities that did not get fixed; 80% of urgent cross site scripting flaws and 70% of urgent SQL injection flaws remained unresolved during the year-long study.<sup>13</sup>

So, even with the best of intentions, code reviews generally aren't realistic as the primary way of securing applications. In the face of market pressures, companies simply don't have the time or resources to do them.

## Centralized Web Application Firewalls

Web Applications Firewalls (WAFs) provide a practical way to augment code reviews, providing a broad blanket of application protection by filtering all incoming Web requests. Unlike traditional network firewalls, WAFs have the ability to understand Web traffic payloads through their Deep Packet Inspection capabilities. They are typically deployed as hardware appliances that sit behind the enterprise firewall and in front of the Web servers.

While WAF appliances can be very effective, they demand significant resources for deployment and management, as they often involve changes to the existing network architecture and they can be difficult to scale across large deployments.

Capacity planning is another challenge, as WAF appliances require an up-front CAPEX investment based on estimates of peak traffic flow. This overprovisioning results in expensive infrastructure that sits under-utilized most of the time, while underprovisioning can result in completely application failure.

Finally, companies must also purchase and manage failover boxes since the WAF appliances are deployed inline, producing a single, critical point of failure. If the firewall fails, the entire site fails—or, at the very least, lies completely vulnerable to attack.

## Akamai WAF: A Distributed Approach to Web Application Security

Akamai's distributed Web Application Firewall (WAF) service offers a unique approach to securing Web applications against pervasive, modern-day threats, leveraging the flexibility and scalability of the Internet cloud to overcome the limitations of more rigid, centralized WAFs. Running as a service deployed across the 50,000-server EdgePlatform, Akamai WAF offers the industry's only distributed web application firewall, combining unmatched scalability, reliability, and performance with ease of integration and simplified management.

Akamai WAF keeps malicious traffic away from the origin Web infrastructure by stopping attacks at their source, at the edges of the Internet. In addition, the service scales automatically, on-demand, offering the capability to defend against today's massive-scale attacks without worry.

### How Akamai WAF Works

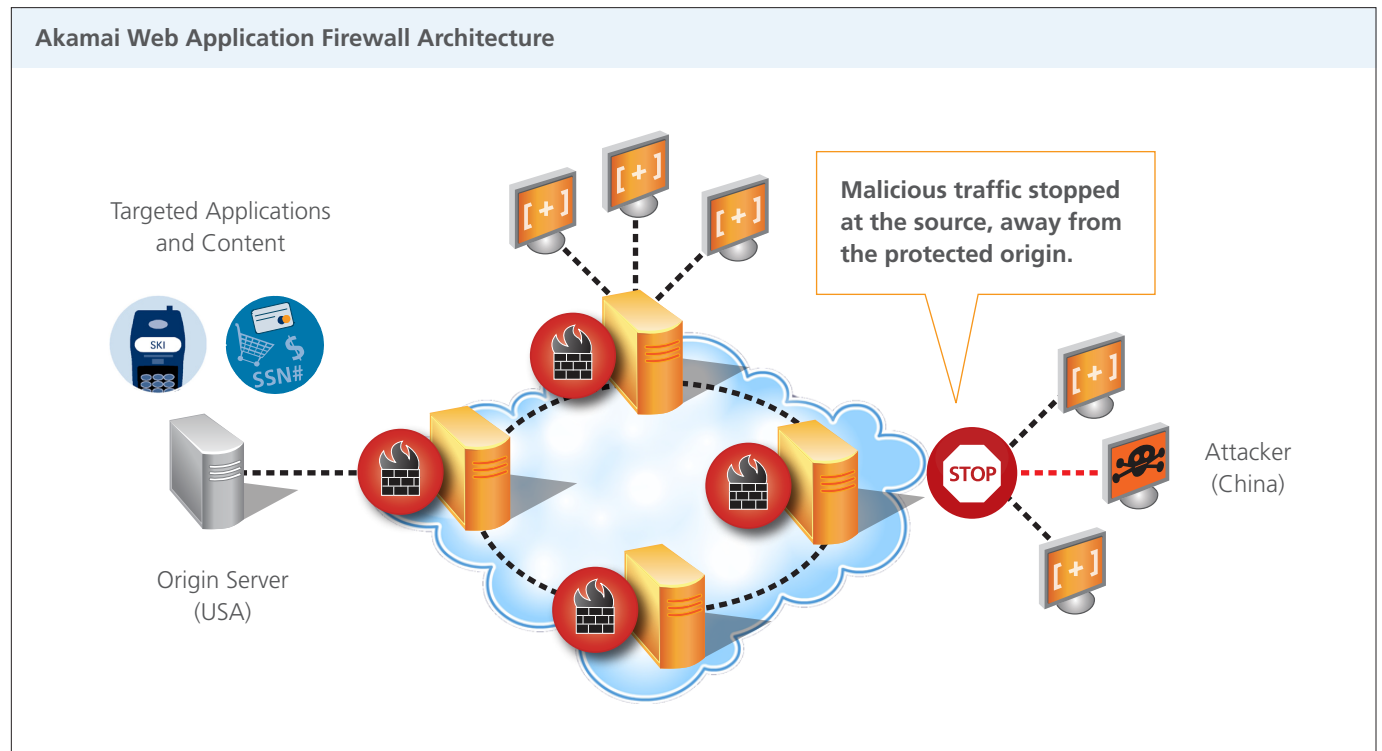
Akamai Web Application Firewall WAF detects attacks by filtering incoming HTTP and HTTPS traffic, based on configurable network and application layer controls. Performing its inspections at the edge of the Internet before Akamai serves each request, WAF can either block or send alerts for any malicious traffic detected. Akamai then responds to legitimate requests by delivering offloaded content and applications directly from the edge, communicating with the origin server as needed.

By focusing on generic attack payload identification rather than attack-specific signature detection, Akamai WAF delivers plug-and-play protection against a broad set of attacks, including zero-day and unknown vulnerabilities. Its core security parameters are based on ModSecurity, a trusted and proven industry-standard

rule set that provides performance-optimized, out-of-the-box security against major exploitation techniques including SQL Injection, Cross Site Scripting, Buffer Overflow, HTTP Response Splitting and other Web-based attacks. The core rule set also defends against malicious bots and security scanners, as well as attempts to access Trojans and backdoors that may have infected the system.

### Distributed WAF Architecture

While WAF protects against the most common threats, not every type of Web application attack is best dealt with this way. Some sophisticated types of attacks require more detailed knowledge of the specific applications and network infrastructure involved and therefore may be best handled at origin. Thus, WAF provides a highly flexible and efficient outer defense layer that works either as a stand-alone firewall or in concert with an enterprise's existing Web application security infrastructure—enhancing the robustness and scalability of that infrastructure by offloading the more generic functions to the Akamai platform. The centralized defenses are then freed up to focus on more application-specific protections.



## Akamai WAF Benefits

Unique in its cloud-based, distributed architecture, Akamai WAF offers a number of key technical, operational, and business benefits to enterprises looking to secure their Web applications in a cost-effective and scalable way.

### The EdgePlatform Advantage

Akamai WAF runs on the EdgePlatform, a time-tested network that has transformed the Internet into a robust and reliable platform for conducting business. By leveraging this proven platform, WAF provides the same types of performance, scalability, availability, and efficiency benefits for Web security infrastructure as Akamai's site delivery services have consistently delivered for Web application infrastructure over the last decade.

WAF is enabled across the 50,000-plus servers in Akamai's global network that deliver approximately one-fifth of the world's Web traffic each day. This means massive distributed firewall capacity is available on demand, eliminating the planning headaches that are associated with scaling out centralized infrastructure.

Moreover, the redundancy and resiliency of the distributed EdgePlatform ensure that WAF protective layer is always available—in contrast to centralized firewalls that create a single point of failure, and require the purchase and management of backup appliances. With WAF, failover is automatic and built in, so that the origin remains always protected.

Because every component of the Akamai platform is optimized for speed, WAF delivers security without a performance hit. In practice, WAF customers have seen no degradation in response times, even with firewall configurations that require over 100 security filters applied to each request. WAF protects their applications while continuing to deliver the full acceleration benefits of the EdgePlatform.

Finally, WAF deals with both legitimate and attack traffic at the edges of the Internet, where it can be most efficiently handled. By detecting and deflecting malicious requests near their source, the origin is protected and attack traffic is kept from crossing the Internet. This unique, distributed approach complements the enterprise's existing centralized security infrastructure to provide a robust, defense-in-depth architecture.

## Operational Advantages

Because it is integrated seamlessly into Akamai's site and application delivery services, Akamai WAF offers the benefits of immediate protection without the hassles of coding, integration, complex rule configuration, appliance deployment, or site re-architecting. It can be implemented quickly and easily, and its optimized core rule set works out-of-the-box so that enterprises can begin benefiting right away.

Finally, as a cloud-based, managed service, Akamai WAF reduces the burden placed on centralized security resources and personnel, enabling a more agile and streamlined core infrastructure that can focus on more customized, application-specific issues.

### Key Technical and Operational Advantages of Akamai WAF

- Robust, proven protection right out of the box
- Massive, on-demand scalability – no more capacity planning headaches
- Superior, built-in availability and performance
- Quick, easy deployment and simplified management
- Attacks deflected at the edge of the network, far away from the origin

## Business Benefits

Akamai WAF's central feature is its transparent delivery of robust application security, helping enterprises to preserve their brand and customer trust by mitigating the risks of business data theft and system compromise. WAF also promotes compliance with regulatory requirements such as PCI DSS section 6.6.

Equally important, however, is the fact that WAF delivers this protection in a flexible and cost-effective way that makes sense for the business bottom line. With its on-demand services model, WAF reduces up front capital investments and eliminates the expensive overprovisioning of security hardware and software. WAF customers also save on costly expenditures for support contracts and upgrades for their security solutions, enjoying a lower total cost of ownership by leveraging the efficiencies of scale built into the EdgePlatform network.

Finally, WAF reduces resource wastage caused by malicious traffic. By stopping attacks at their source, at the edges of the Internet, WAF cuts the costs associated with bandwidth and other origin resources that would otherwise be consumed by the attacks.

### Key Business Benefits of Akamai WAF

- Protect branding and revenue by mitigating risks associated with system compromise
- Promote compliance with PCI and other regulatory requirements
- Reduce capital expenditures, maintenance overhead, and total cost of ownership
- Avoid costly overprovisioning and resource wastage due to attack traffic
- Offload and streamline in-house security resources

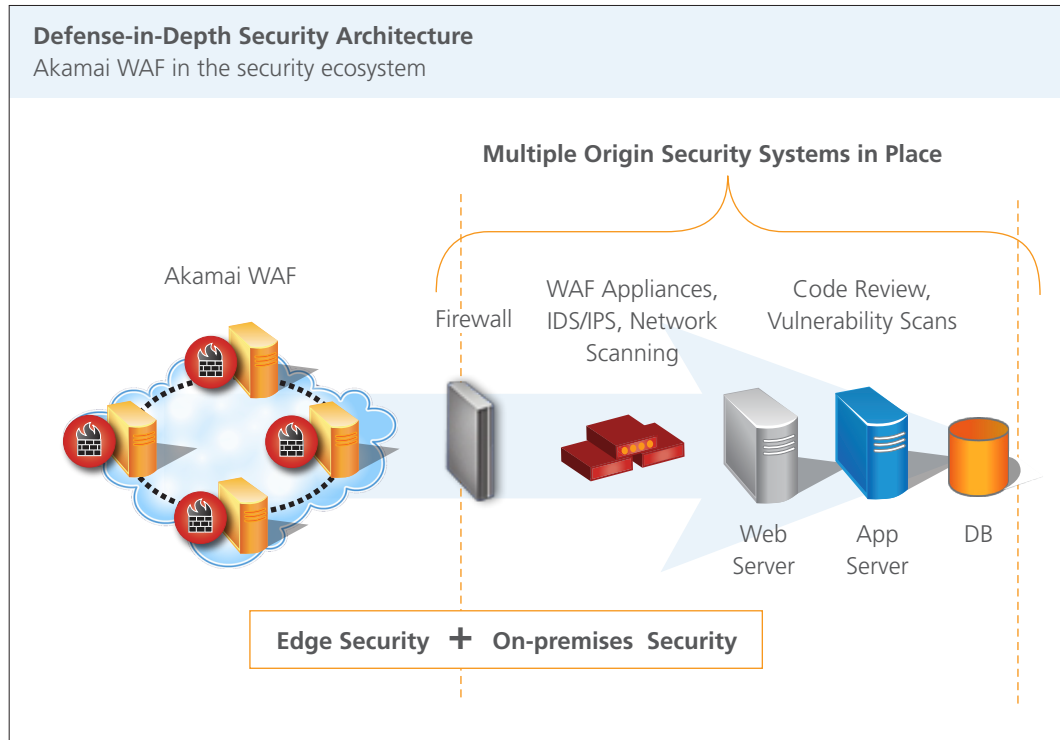
## Defense-in-Depth with Akamai WAF

Modern-day security best practices dictate a defense-in-depth approach that makes use of a diverse set of tools to create overlapping layers of protection for the porous enterprise perimeter. In order to combat threats of the complexity and severity we see today, a defense-in-depth architecture must augment traditional, centralized solutions, like firewalls and intrusion prevention systems, with a new breed of distributed, cloud-based security services, like Akamai WAF, as shown in the architecture diagram below.

Within such an architecture, Akamai WAF delivers a robust and cost-effective outer defensive ring that complements existing centralized security controls. It offloads and bolsters these centralized security resources while providing the additional scalability and reach needed to defend an enterprise perimeter that now extends to the edges of the Internet. The result is a streamlined origin infrastructure, augmented by a flexible, on-demand outer layer—together providing vigorous application defenses while reducing IT planning and maintenance headaches.

**An effective Defense-in-Depth architecture for application protection combines multiple security layers, including:**

- Traditional, centralized firewalls
- Intrusion detection/Intrusion prevention
- Network Scanning
- Secure coding and code reviews
- Vulnerability scans
- Distributed WAF for protection at the edge



## About Akamai Security

For over ten years, the world's leading businesses have leveraged Akamai's proven, secure, and highly fault-tolerant platform to accelerate their mission-critical transactions over an insecure Internet. With thousands of companies depending on the EdgePlatform to reliably deliver 500 billion Web interactions each day, security is always at the forefront at Akamai. It is comprehensively integrated into every aspect of Akamai's network and operations, to protect not only Akamai and its customers, but also the Internet at large. Thus, with its proven security expertise, unmatched global purview, and massively distributed network, Akamai is uniquely able to help businesses harness the power of the Internet—and defend their perimeters against its evolving, wide-scale threats.

<sup>1</sup> Symantec's Internet Security Threat Report, April 2009, puts the percentage at 60%, while Cenzic's Web Application Security Trends Report, Q3-Q4 2008, puts it at 80%, based on data compiled from multiple third-party threat databases.

<sup>2</sup> <http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jul-2009-na-wpus.pdf>

<sup>3</sup> [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_underground\\_economy\\_report\\_11-2008-14525717.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf)

<sup>4</sup> [http://www.mcafee.com/us/about/press/corporate/2009/20090129\\_063500\\_j.html](http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html)

<sup>5</sup> [http://www.websense.com/site/docs/whitepapers/en/WSL\\_Q1\\_Q2\\_2009\\_FNL.PDF](http://www.websense.com/site/docs/whitepapers/en/WSL_Q1_Q2_2009_FNL.PDF)

<sup>6</sup> <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>, <http://www.fas.org/sgp/crs/terror/RL32114.pdf>

<sup>7</sup> <http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>

<sup>8</sup> <http://projects.webappsec.org/Web-Application-Security-Statistics>

<sup>9</sup> <http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf>

<sup>10</sup> <http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=2#sID200>

<sup>11</sup> [http://www.whitehatsec.com/home/assets/WPstats\\_spring09\\_7th.pdf](http://www.whitehatsec.com/home/assets/WPstats_spring09_7th.pdf)

<sup>12</sup> [http://www.cenzic.com/downloads/Cenzic\\_AppSecTrends\\_Q3-Q4-2008.pdf](http://www.cenzic.com/downloads/Cenzic_AppSecTrends_Q3-Q4-2008.pdf)

<sup>13</sup> [http://www.whitehatsec.com/home/assets/WPstats\\_spring09\\_7th.pdf](http://www.whitehatsec.com/home/assets/WPstats_spring09_7th.pdf)

<sup>14</sup> For more information, see the Akamai Information Security Management System Overview, which discusses Akamai's comprehensive network and operational security policies in greater detail.

## The Akamai Difference

Akamai® provides market-leading managed services for powering rich media, dynamic transactions, and enterprise applications online. Having pioneered the content delivery market one decade ago, Akamai's services have been adopted by the world's most recognized brands across diverse industries. The alternative to centralized Web infrastructure, Akamai's global network of tens of thousands of distributed servers provides the scale, reliability, insight and performance for businesses to succeed online. Akamai has transformed the Internet into a more viable place to inform, entertain, interact, and collaborate. To experience The Akamai Difference, visit [www.akamai.com](http://www.akamai.com).

### Akamai Technologies, Inc.

#### U.S. Headquarters

8 Cambridge Center  
Cambridge, MA 02142  
Tel 617.444.3000  
Fax 617.444.3001  
U.S. toll-free 877.4AKAMAI  
(877.425.2624)

[www.akamai.com](http://www.akamai.com)

#### International Offices

Unterfoehring, Germany	Bangalore, India
Paris, France	Sydney, Australia
Milan, Italy	Beijing, China
London, England	Tokyo, Japan
Madrid, Spain	Seoul, Korea
Stockholm, Sweden	Singapore



©2009 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice.