

The Business Case for Web Application Firewalls

Ken Tyminski
For Breach Security, Inc.

September 2007



OVERVIEW

As a leader in your organization's information technology department, you make sure that your technology strategy is aligned with business needs. Often, however, those two areas end up on opposite sides of the spectrum, particularly where security is concerned.

Consider the case of web applications. Your organization may be deploying them to increase revenues, decrease transaction costs, and improve customer service levels. To secure them, you may be planning to implement secure coding practices, hire a vulnerability scanning vendor to review your application, and deploy network intrusion detection/intrusion prevention systems (IDS/IPS) or other security technologies.

Yet, what will you do when the executive team or sales and marketing departments say: "we need to add this new feature, but the web application must still be live on the original date"? Do you compromise your technology strategy and deploy the application on time, but with less rigorous testing and security measures? Or, do you make the case that, although delaying the "go live" date may mean missed revenue opportunities, it will be more beneficial for the organization in the long run?

If this situation sounds familiar, a web application firewall may provide the solution.

WEB APPLICATION FIREWALL MARKET DRIVERS

Web applications are inherently vulnerable. Before the question was *whether* an organization's web applications would be attacked. Now the question is *when* the attack will occur. Recent studies support this trend. An increasing amount of the new vulnerabilities discovered are designed to take advantage of web application and web browser flaws. The majority of these vulnerabilities are easily exploitable. Web applications and browsers were written at a specific point in time, often years ago, before many of the exploitative techniques used by hackers today were invented.

Web application vulnerabilities can impact compliance. Organizations cannot afford to have vulnerabilities in their web applications. Government and industry have become involved in ensuring the protection of individuals' sensitive information online. The laws and standards they have enacted do not distinguish between an accidental data leak to an authorized user and a security exploit that allows a hacker into a web application's database—non-compliance is not a matter of degree.

Non-compliant organizations can face substantial fines and higher transaction fees, in addition to remediation costs. In the case of an actual security incident, non-compliant organizations may see multiple quarters of substantially decreased revenues due to customer defections. On the other side, organizations that comply with regulations in advance of deadlines may receive significant financial bonuses.

Web applications must be available 24 x 7 x 365. Web applications need maximum up-time to reach the Internet's worldwide audience. Organizations cannot afford to take down their web applications to fix issues found after deployment or add new features. Offline web applications do not bring in revenue and may **cost** money in the form of service-level agreement penalties.

Web applications are difficult and costly to fix. Most organizations have multiple web applications deployed. For large organizations in particular, that number can range from a few hundred to several thousand applications. There is usually too much code and not enough skilled developers to fix web application issues while continuing work on new releases. For third-party commercial or custom web applications, issue resolution becomes even more difficult, as the organization is at the mercy of the vendor's schedule and its internal development capabilities.

CURRENT SOLUTIONS

The table below shows a list of the solutions many organizations have implemented to protect their web applications and outlines the pros and cons of each approach.

Solution	Pros	Cons
Secure Coding Initiatives	<ul style="list-style-type: none"> • A recommended best practice. • Adds security up front in the development process. 	<ul style="list-style-type: none"> • Coding is done by people and people can make mistakes. • Can be costly if outsourced and testing must still occur in-house. • Must be repeated for every subsequent release.
Vulnerability Scanning	<ul style="list-style-type: none"> • A recommended best practice. • May allow organizations to discover vulnerabilities quicker than a line-by-line code review. 	<ul style="list-style-type: none"> • Takes a snapshot of the web application at a point in time. <ul style="list-style-type: none"> – When the code changes, the application is no longer secure. • May not scan every line of code in the application for issues. • May generate inconsistent findings. • Does not fix the issues found. • Can be costly for organizations with multiple web applications.
Network IDS/IPS Deployment	<ul style="list-style-type: none"> • A recommended best practice. • Protects network resources. 	<ul style="list-style-type: none"> • Cannot prevent new and unique attacks (as is often the type conducted against web applications), only known attacks. • Does not protect against web application security defects caused by poor coding.

Current Web Application Security Options

THE BENEFITS OF WEB APPLICATION FIREWALLS

Because of the limitations of secure coding initiatives, vulnerability scanning, and IDS/IPS's with respect to web application security, many organizations have deployed web application firewalls to complement their security efforts. A web application firewall is hardware with embedded software that is designed specifically to protect an organization's web applications and servers from attack and information leaks. To accomplish this, web application firewalls use two security models. A positive security model allows "good" web traffic to flow into an out of the web application. A negative security model ensures that "bad" traffic is blocked before it comes into the network and sensitive information is prevented from disclosure through the application.

The two security models allow web application firewalls to protect organizations against **both known and new web** application attacks. In addition to providing increased security, web application firewalls offer a variety of business benefits.

- **Rapid deployment of web applications.** A web application firewall acts as a “virtual patch” for all of its protected web applications, providing continuous security that shields vulnerabilities against exploit. With a web application firewall, organizations can accelerate their time to market, as they can still deploy those applications with known vulnerabilities. They can then enjoy the benefits of the “first-mover advantage” while the development team continues to remediate issues.
- **Significant cost savings.** A one-time deployment of a web application firewall can reduce the frequency with which an organization needs to scan for vulnerabilities. If the web application firewall has the ability to dynamically learn and adjust its protection, additional scanning passes for each code change can be minimized. Organizations with multiple or highly dynamic applications can see their web application firewall investment paid back from the scanning cost savings alone.
- **Increased coordination between the security and development teams.** In many organizations, a disconnect exists between the security and development teams. Completed web applications are often “thrown over the wall” to the security team for implementation in a production environment. As a result, the security team many have little knowledge of the application it is responsible for protecting. A web application firewall can provide the security team with the knowledge it needs. By extending the security team’s understanding, the web application firewall enables it to communicate issues more clearly to development.

THREE KEY QUESTIONS TO ASK WHEN LOOKING AT WEB APPLICATION FIREWALLS

If you decide to deploy a web application firewall in your organization, you will want to ask your prospective vendors these three questions:

1. **Has the technology been proven in real-world environments?** The web application firewall should be deployed successfully in referenceable organizations. The deployments should also be able to clearly demonstrate that they address the same security and regulatory challenges that your organization faces.
2. **Does the product support or impede business operations?** The web application firewall should be transparent to application users and not interfere with their ability to complete transactions online. Additionally, the web application firewall should fit into your network without introducing another point of failure that could disable the protected applications.
3. **Does the product provide actionable information that can be used by the security, development, and testing teams?** The web application firewall should provide a comprehensive picture of each protected application that gives your security team a thorough understanding of transactions and the context in which they operate. Furthermore, the web application firewall should provide enough detail about vulnerabilities and application security defects so the development and testing teams can easily understand the steps they need to take to fix issues.

WHY YOU SHOULD CONSIDER THE WEBDEFEND™ WEB APPLICATION FIREWALL

The Breach Security™ WebDefend web application firewall not only meets all of the criteria mentioned above, but also includes unique capabilities that help organizations save time, money, and increase internal coordination:



- **Successful deployments in a variety of organizations.** WebDefend has been deployed in all sizes of organizations, as well as educational institutions and government agencies. Some of its satisfied customers include Bayer Pharmaceuticals, Sovereign Bank, and Sacred Heart University.

- **Non-intrusive deployment and security.** WebDefend deploys out-of-line and does not introduce latency or a single point of failure into the network. Its out-of-line deployment ensures that its security is non-intrusive to protected web applications and transparent to users.
- **Detailed, actionable information that can be used by security and development teams.** WebDefend includes an instructive console which helps security teams understand the content in which events are generated and remediate problems quickly. For every event detected, a detailed text description is included with the actual transaction, information about the vulnerability, related compliance issues, and links to online resources. Powerful reporting tools help communicate web application security issues to development and meet compliance requirements.

In addition, WebDefend includes a number of features not found in other web application firewalls:

- **Application security defect detection.** WebDefend passively monitors protected applications to detect and report on security defects. By continuously monitoring the web applications, WebDefend ensures that defects are discovered in real time. Assessing the web applications in their actual environments allows WebDefend to identify defects that might otherwise go unnoticed during a vulnerability scan or code review.
- **Email help ticketing for application security defects.** WebDefend allows security teams to create email help tickets for development and testing teams simply by right-clicking on an individual defect listing. Help ticket emails include a full description of the defect, detailed instructions on how to remediate it, reference links for further information, and a sample request and reply to demonstrate the issue. This comprehensive information enables the teams to communicate in a common language, saving valuable development time and ensuring a better quality of releases.
- **Payment Card Industry Data Security Standard-specific rule sets and reports.** WebDefend includes pre-packaged rule sets specifically designed for organizations working to comply with the Payment Card Industry Data Security Standard (PCI DSS). These rules ensure the proper configuration of security mechanisms for attack prevention as well as audit logging of all payment card usage for PCI compliance. PCI-specific reports provide an immediate view of the system's overall level of compliance as well as details of sensitive information use for audit purposes.
- **Automated application profiling with change detection.** WebDefend's patent-pending Adaption™ technology understands the context of each protected application, building customized, individual profiles of "acceptable" behavior. When a web application changes, WebDefend automatically updates the profile so security teams can focus on protecting applications instead of configuring tools.
- **Inbound and outbound traffic analysis.** Only WebDefend includes the patent-pending ExitControl™ traffic analysis engine that inspects both incoming and outgoing traffic to prevent application defacement, block informative error messages, and preempt data theft. Pre-defined and customizable BreachMarks™ within the ExitControl engine represent patterns that define a specific type of information, such as credit card or Social Security numbers. WebDefend allows organizations to set BreachMark policies to alert on and prevent matching information from leaving the organization.

SUMMARY

Web application firewalls offer a variety of business benefits such as rapid application deployment, significant cost savings, and increased communication between development and security teams. In addition, they also provide security advantages that complement secure coding initiatives, vulnerability scanning efforts, and

network IDS/IPS's. As a result, a web application firewall should be a critical component of your web application security strategy. Breach Security's WebDefend web application firewall supplies you with the proven technology and capabilities you need to ensure that this piece of your security strategy is aligned with your business needs.

ABOUT THE AUTHOR

Ken Tyminski has over 32 years of information technology experience, most recently serving as Vice President and Chief Information Security Officer for the Prudential Insurance Company of America. In this position, he was responsible for ensuring that Prudential's business systems were architected appropriately, implemented securely, and protected from malicious outsiders and insiders. As CISO, he also led the Information Security Office for Prudential, which established policies and standards and ensured controls were in place for millions of users, thousands of branches, and hundreds of offices across the country and internationally.

Prior to his assignment as Prudential's first Chief Information Security Officer, Ken held several other prominent positions. While working in the Corporate Technology Services organization, he managed the Operations Control Center, overseeing the entire technology operation for the enterprise. Ken has also managed Information Technology Help Desks, IT Controls and Compliance functions, Technology Research, and Software Engineering organizations. Ken graduated Magnum Cum Laude from Upsala College with a BS degree in Business Administration. He also earned a certificate in Electrical Engineering Technology from the New Jersey Institute of Technology.

ABOUT BREACH SECURITY

Breach Security, Inc. is the leader in protecting organizations and their customers from attacks intended to compromise sensitive information such as credit card numbers and human resources records from their websites. With the best attack detection for web application threats at the lowest total cost of ownership in the industry, the company's web application firewalls are the most widely deployed in the world. Breach Security provides web security solutions to Fortune 100 companies and enterprise customers such as Bayer Pharmaceuticals, Sovereign Bank, and SAP. Founded in 2004, Breach Security is a privately-held company based in Carlsbad, California.



Castleforce IT Consultancy Ltd
Enterprise Centre, University of Reading
L33 London Road Campus
London Road, Berkshire, RG1 5AQ
tel (north): 0151 203 1400
tel (south): 0118 9071600
info@castleforce.com



Breach Security, Inc.
Corporate Headquarters
2075 Las Palmas Drive
Carlsbad, CA 92011
tel: 760-268-1924
toll-free: 866-205-7032
info@breach.com