

Organizations of all sizes are potential targets of data security incidents. With recovery costs reaching \$22 million in some cases, they can be fatal blows.

— The Ponemon Institute  
"2006 Annual Study: Cost of a Data Breach"  
October 2006

## Comprehensive Web Application Security

*The WebDefend web application firewall appliance goes beyond vulnerability scanning efforts, secure coding initiatives, and network security solutions by providing organizations with continuous, real-time web application-specific security.*

WebDefend is an advanced web application firewall that offers customized, behavior-based security for each protected application. Only WebDefend uses a patent-pending profiling system and multiple, collaborative detection engines to ensure the flow of mission-critical traffic while supplying complete protection for applications to keep the organization's confidential information safe from targeted attacks and leaks. Deployed out-of-line, WebDefend uniquely provides non-intrusive, effective security for multi-application environments while continuing to provide full blocking capabilities.

### Key Features

#### Dynamic Application Profiling

The patent-pending Adaption™ profiling system automatically builds a customized, positive security model of each protected application to understand its acceptable behavior. The system maps all levels of application behavior, so there is no need for detailed knowledge or secure coding. As the application is updated, WebDefend automatically detects the changes, learns them, and adjusts the profile.

#### Inbound and Outbound Traffic Analysis

Only WebDefend offers inbound and outbound traffic analysis through the patent-pending, bi-directional ExitControl™ traffic analysis engine. ExitControl inspects both incoming and outgoing traffic to block hacker-informative error messages and prevent application defacement and 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. Organizations can set BreachMark policies to alert on and prevent the loss of matching data.

#### Application Security Defect Detection

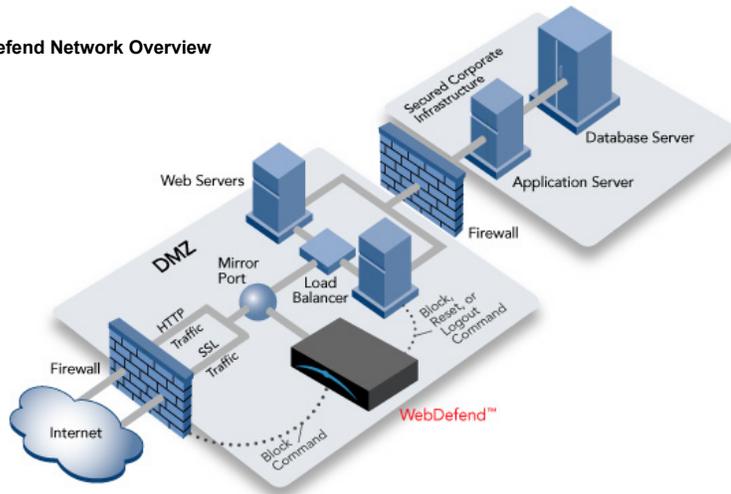
WebDefend uniquely identifies and reports on application security defects caused by insecure coding techniques. These defects, such as missing images or hyperlinks and improper request handling, negatively impact the user experience by preventing application access or disabling the web server. Each protected application is passively monitored for anomalies in its responses. If necessary, corresponding inbound request are analyzed to determine underlying causes. By assessing an entire application in its actual environment, WebDefend pinpoints defects that would otherwise go undiscovered during a code review or vulnerability scan.

#### Out-of-the-Box PCI Compliance

WebDefend includes pre-packaged rule sets designed specifically 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 the logging of all payment card usage for 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.

(continued)

## WebDefend Network Overview



### Key Features (continued)

#### Full Monitoring and Blocking Capabilities

A full suite of monitoring and blocking capabilities allow organizations to customize WebDefend's response to threats. A simulation mode facilitates deployment by indicating what WebDefend would prevent, without requiring full blocking functionality to be enabled.

WebDefend's blocking capabilities range from logging out malicious users, integrating with popular web servers for attack blocking and network firewalls for IP blocking, and TCP resets.

#### SSL Attack Detection

WebDefend replicates and decrypts SSL traffic streams without terminating the original encrypted session. Immediately after decryption, WebDefend inspects the traffic entering and leaving the web environment, providing full visibility and attack detection capability without compromising performance.

**Intuitive Management Console** The easy-to-use WebDefend Management Console provides a single point of sensor configuration and management. Organizations can immediately use the console, without any initial training, to gain full visibility into their web applications' architectures and security. The instructive console helps organizations understand the context in which events are generated and remediate problems quickly. For every event detected, a detailed description pinpoints the vulnerability, offers insight into its meaning, and assists with its resolution. The console offers multiple event views, allowing organization to examine entire transactions and see the error messages presented to users. Events can also be filtered, so only exceptions are shown. Powerful reporting tools help communicate web application security issues to development, meet compliance requirements, and track the effectiveness of WebDefend policies.

### Benefits

- Provides real-time, continuous web application security.
- Delivers non-intrusive and effective security—WebDefend is the only sensor that deploys out-of-line and blocks 100% of detected attacks.
- Automates web application compliance to regulations and industry standards, such as the PCI DSS.
- Detects security defects that vulnerability scans miss, by passively monitoring web application traffic.
- Bridges the gap between security and development teams with detailed reporting on sources of vulnerabilities for quick remediation.

### 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 web sites. 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.

For more information, please visit our web site at [www.breach.com](http://www.breach.com).

### COMPLIMENTARY SOLUTIONS

#### WebDefend Manager

The WebDefend Manager appliance is designed to support organizations with distributed or multi-sensor environments. The WebDefend Manager consolidates security events and defects from all protected applications and centralizes command and control for remote sensors.

#### High Availability Deployment Option

The high availability deployment option provides redundancy in web application security and is recommended for organizations with a critical need for uninterrupted protection. Compatible with any network, this option provides constant web application security across geographically distant data centers.

### SERVICE OPTIONS

- Standard Support includes email and phone support from Monday through Friday, 8 a.m. to 5 p.m. Pacific, plus all product maintenance updates.
- Premium Support includes 24 x 7 x 365 email and phone support, next-day replacement service, and all product maintenance updates.
- On-site installation, extended hardware coverage, and professional services are also available.

*Additional charges may be required.*

**BREACH**

Breach Security, Inc.  
Corporate Headquarters  
2075 Las Palmas Drive  
Carlsbad, CA 92011  
Phone: +1 760 268 1924  
Toll-Free: +1 866 393 0907  
Fax: +1 760 454 1746  
[www.breach.com](http://www.breach.com)