

WEBDEFEND®

The WebDefend web application firewall appliance provides web applications with real-time, continuous security against attacks and data leakage, ensure they operate as intended and help them comply with industry regulations such as the Payment Card Industry (PCI) Data Security Standard (DSS).

Using bi-directional traffic analysis, automated behavioral profiling and multiple collaborative detection engines WebDefend also identifies web application issues that can affect their security, functionality and availability. WebDefend maintains the flow of business-critical traffic while delivering complete protection for payment card data, Social Security numbers and other sensitive information.

BENEFITS

- Provides unparalleled data leakage protection for sensitive information.
- Supports multi-application environments across multiple data centers with minimal effort.
- Facilitates compliance with PCI DSS Requirements 2, 3, 4, 5, 6, 7, 8, 10, 11 and 12.
- Allows organizations to identify application issues that jeopardize revenue, diminish the customer experience and threaten the security of sensitive information.
- Enables quality discussions and timely communications between security, development and management teams.
- WebDefend Global Event Manager enables customers to make distributed cloud and data center defense-in-depth architectures operational.

KEY FEATURES

Unparalleled Attack Detection and Prevention

WebDefend provides the industry's best detection of and protection against existing vulnerabilities and emerging threats such as site scraping, malicious bots, Google™ hacking and zero-day and targeted attacks.

To achieve comprehensive, accurate protection, WebDefend inspects traffic entering and leaving the web application, correlating the data from multiple attack detection engines:

- The patent-pending Adaption

application profiling system continuously builds a dynamic security model of each protected web application to ensure that only valid traffic is allowed.

- Adaption can profile HTML, XML, and SOAP and WebDefend can monitor uncompressed or compressed web traffic.
- Adaption automatically relearns HTTP constraints along with the existing information it profiles and relearns about individual web application parameters.
- The patent-pending ExitControl traffic analysis engine inspects outgoing traffic for data leakage, defacement and detailed security information.
- The application-layer signatures developed by Breach Security™ Labs provide the industry's most current source of application-specific signatures and actionable information on detected vulnerabilities.

A full suite of monitoring and blocking capabilities allow organizations to customize WebDefend's responses. WebDefend blocks using TCP resets, web server agents, external devices such as firewalls, by logging or locking out users or when deployed in-line.

Robust and Easy Enterprise Implementation

WebDefend is designed for large-scale enterprise deployments. Its multi-tier architecture allows separate protection for and management of multiple data centers. Any sensor can be made redundant for high availability of web application security. WebDefend Managers are available to centralize control of and reporting for multiple or remote data centers.

To ensure non-intrusive, accelerated deployment in a complex, distributed web architecture, WebDefend can be deployed out-of-line or transparently in-line, without requiring any network reconfiguration.

WebDefend



"Five out of five stars."

SC Magazine
January 2009

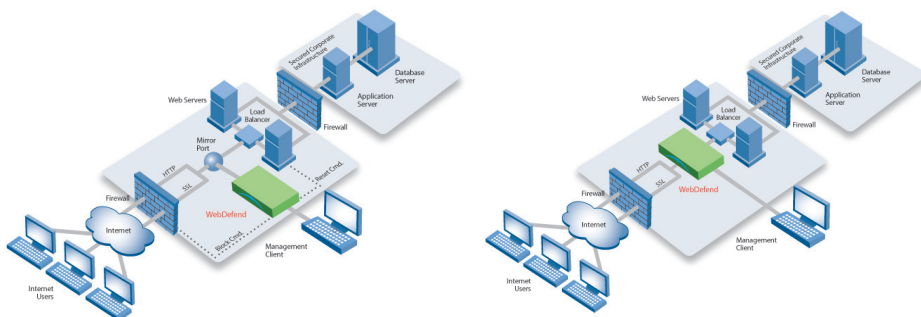
"There's no doubt that [WebDefend] is an excellent solution for PCI compliance."

Information Security Magazine
March 2008

"If you are using active web content such as online banking applications, you cannot afford to be without this product."

SC Magazine
February 2008

Typical WebDefend Deployment



Out-of-the-Box PCI Compliance

WebDefend includes a pre-packaged PCI policy and reports for organizations working to comply with the PCI DSS. The PCI policy ensures the proper security configuration for attack prevention and the logging of all payment card use. PCI-specific reports provide an immediate view of a web application's overall level of compliance and details of sensitive information use for audit purposes.

Immediate Integrity and Security Issue Detection

WebDefend performs a continuous assessment of each protected application to identify issues that can impact the application's security, functionality and availability. Issues include programming mistakes, application errors or failures and insecure code.

When an issue is discovered, WebDefend captures the full request and response, as well as a browser view, so the problem can be easily understood and remediated.

Intuitive, Instructive Console

The easy-to-use WebDefend Management Console provides a single point of configuration and monitoring. Administrators can immediately use the console, without prior training, to gain a complete understanding of web application architectures and security.

The console helps organizations understand the context of events and remediate issues quickly. For every event or defect detected, a detailed description pinpoints the problem, offers insight into its meaning and explains its resolution. The console offers multiple event views and drill-down capabilities, allowing administrators to identify events easily, examine root causes, view entire transactions and see error messages presented to site visitors.

Powerful reporting tools communicate security issues to application development and executive management, help meet

compliance requirements and track the effectiveness of WebDefend policies.

Dashboard

WebDefend features a system level dashboard providing a flexible summary overview of the security throughout protected web application environments along with real-time status reporting on all systems in a WebDefend deployment.

Web Application Performance Monitoring

WebDefend provides users with real-time visibility into the performance of their web applications. WebDefend Application Performance Management identifies problems and trends at the site, URL and session levels in your web application environment with out-of-the-box real time views covering performance metrics such as transaction time, error rate, availability and HTTP and HTTPS throughput. Because WebDefend automatically profiles web applications, operators do not need to define application structures or paths.

Performance Monitoring improves ROI by enabling issue identification, maintenance and operational planning, vendor management, and internal charge backs associated with specific web applications.

ABOUT BREACH SECURITY™

Breach Security, Inc. is the leading provider of real-time, continuous web application security that protects sensitive web-based information. Breach Security's products protect web applications from hacking attacks and data leakage and ensure applications operate as intended. The company's products are trusted by thousands of organizations around the world, including leaders in finance, healthcare, ecommerce, travel and government.

For more information, contact your authorized Breach Security representative or visit www.breach.com.

TECHNICAL SPECIFICATIONS

- Protected protocols: HTTP, HTTPS, (SSL), XML, web services, SOAP and AJAX.
- Pre-defined policies: Default, PCI Compliance, Hosting and Audit.
- Alerting and monitoring options: email, syslog, SNMP custom alerts, event viewer, dashboard and integrated reporting.
- Blocking options: in-line deployment, TCP reset, web server agent, user logout, firewall and other devices.

OPTIONAL MODULES

WebDefend Manager

The WebDefend Manager consolidates security events and defects and provides centralized control for multiple local or remote sensors.

High Availability Option

The high availability deployment option provides local and data center redundancy for sensors and WebDefend Managers to ensure continuous web application security.

WebDefend Global Event Manager (GEM)

Enables real-time monitoring and analysis of events from the Akamai WAF Service and ModSecurity along with WebDefend events in the management console and help make distributed cloud - data center defense in depth architectures operational.

SERVICE OPTIONS

- Standard Support includes email and phone support during local business hours, plus all product maintenance updates.
- Premium Support includes 24x7x365 email and phone support, a one-year hardware warranty, next-day replacement service and all product maintenance updates.
- On-site installation, extended hardware coverage and professional services are also available.



Breach Security, Inc.
Corporate Headquarters

2141 Palomar Airport Road, #200 | Carlsbad, CA 92011 | USA
tel: (760) 268-1924 | toll-free: (866) 205-7032
fax: (760) 454-1746 | www.breach.com