TRUSTWAVE WEB APPLICATION FIREWALL

CONTINUOUS WEB APPLICATION PROTECTION

Award-winning Trustwave Web Application Firewall is highly scalable and provides real-time, continuous security against attacks and data loss with the assurance that your Web applications operate as intended and are compliant with industry regulations.

Trustwave's Web Application Firewall offers customized, behavior-based security for each protected application and is integrated with our award-winning Trustwave SIEM, which correlates and consolidates attack information from many sources beyond Web applications.

The Trustwave Web Application Firewall, implemented as a physical or virtual on premise appliance or as a managed security service, provides virtual patching to protect your vulnerable applications from attack, without having to wait for the next release cycle. Only Trustwave's Web Application Firewall 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 your confidential information safe from targeted attacks.

KEY FEATURES

Trustwave's Web Application Firewall provides the industry's best protection against application vulnerabilities and emerging threats, such as OWASP Top 10 Web application attacks, site scraping, malicious bots, GoogleTM hacking, zero-day and targeted attacks:

- Patent-pending, adaption application profiling system continuously builds a dynamic security model of each protected Web application to ensure only valid traffic is allowed
- Patent-pending ExitControl analysis engine inspects outgoing traffic for data loss, defacement and security information exposure
- Application layer signatures provide actionable information on detected vulnerabilities
- Geo-location blocking provides customization for blocking requests generated by specific countries
- Highly scalable appliance covers flexible site definitions, flexible deployment modes and support for up to 10G NIC cards
- Facilitates compliance with PCI DSS requirement 6.6
- Provides enhanced virtual patching with user defined rules based on regular expressions syntax
- Custom response page to communicate a response to potential hackers based on the type of attack initiated

Easy Implementation, Robust Performance

Trustwave's Web Application Firewall is designed to scale from single application to global enterprise deployments:

- Multi-tier architecture allows separate protection for and management of multiple data centers
- Appliances can be made redundant for high availability
- Deploy out-of-line or transparently, in-line transparent bridge, without requiring any network reconfiguration, or reverse proxy
- Multi-tenancy allows multiple customers or departments to be defined in a single appliance, ensuring data is not shared across users – ideal for complex organizations and managed security service providers (MSSPs)

The Trustwave Web Application Firewall Manager is optionally available to consolidate security events and defects plus centralize control and reporting of more than one appliance.

Immediate Integrity and Security Issue Detection

Trustwave's Web Application Firewall performs continuous assessment of your protected applications to identify issues that impact the application's security, functionality and availability, including programming mistakes, application errors or failures and insecure code.

Virtual Patching

Virtual patching enables you to apply user-defined rules to quickly address vulnerabilities. When vulnerabilities are identified through regular application scanning, virtual patches immediately protect while your software development team fixes the underlying bug. Virtual patching protects vulnerable applications from attack, without having to wait for the next release cycle. The Trustwave Web Application Firewall integrates with the industry-leading Web application scanners.

TECHNICAL SPECIFICATIONS

- Protected protocols: HTTP, HTTPS (SSL, TLS), XML, Web services, SOAP and AJAX
- 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
- Languages: supports the collection and analysis of Web application traffic in any language, including double-byte character languages
- Supports VLAN IDs
- Supports remote LDAP-2 or LDAP-3-based authentication of console users

Intuitive, Instructive Console

The management console lets you enjoy ease of use with a single point of configuration and monitoring. Immediately use the console, without prior training, to gain a complete understanding of Web application architectures and security.

The console helps you understand the context of events to quickly remediate issues. For every event or defect detected, a detailed description pinpoints the problem, provides insight into its meaning and explains its resolution. The console offers multiple event views and drill-down capabilities, allowing you to easily identify events, examine root cause, 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 Trustwave's Web Application Firewall policies.

Web Application Performance Monitoring

The solutions provide real-time visibility into the performance of your Web applications. The Trustwave Web Application Firewall Application Performance Management identifies problems and trends at the site, URL and session levels in the Web application environment – all with real-time views that provide performance metrics. Because The Trustwave Web Application Firewall automatically profiles Web applications, you do not need to define application structures or paths.

Trustwave®

Smart security on demand

For more information: https://www.trustwave.com

KEY BENEFITS

Trustwave's Web Application Firewall provides unparalleled protection against the loss of sensitive information.

Visibility

Patent-pending profiling system and collaborative detection engines ensure the protected flow of your mission-critical traffic and offer the industry's only correlation of inbound and outbound events and help to maintain application integrity.

Lowest Total Cost of Ownership

Features automatic and continuous profiles of your Web applications that deliver maximum security with minimal management overhead.

Flexibility

Because it is easy to use, security events and vulnerabilities can be identified with an intuitive console that provides a single point of configuration and monitoring in either an on premise appliance (hardware or virtual) or as a managed security service that provides 24x7 analysis from our Trustwave experts.

SERVICE OPTIONS

- Standard Support includes e-mail 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 for Trustwave Web Application Firewall hardware appliance and all product maintenance updates.
- On-site installation, extended hardware coverage and professional services are also available.

MINIMIZE RISK WITH APPLICATION SECURITY LIFE CYCLE SOLUTION

Trustwave 360 Application Security program ensures security is at the very foundation of software development and ongoing operations by providing market-leading, robust services and technologies to protect critical applications and sensitive data, including: developer training, managed security testing for applications, application code review and our Web application firewall solutions – delivering a holistic approach to secure applications.

AWARD-WINNING SOLUTION

Trustwave Trustwave Web Application Firewall has achieved Common Criteria validation with EAL 2+ level of certification.