Trustwave®

DATA SHEET

Trustwave Web Application Firewall

AVAILABLE AS A MANAGED SERVICE OR MANAGE IT YOURSELF

Benefits

- Reduce risk of downtime or data loss resulting from a web application attack
- Reduce costs associated with regulatory or compliance fines
- Temporarily patch applications while developers are fixing vulnerabilities
- Improve customer satisfaction by avoiding attacks, downtime, and data loss
- Improve application performance by sharing web issues and trends with developers

Web applications are increasingly becoming targets of attacks and most include at least one serious vulnerability. In 2017, 99.7% of the applications assessed by Trustwave SpiderLabs did. A web application firewall (WAF) is one of the best controls to help protect your vulnerable web applications, while at the same time addressing compliance requirements like the PCI DSS.

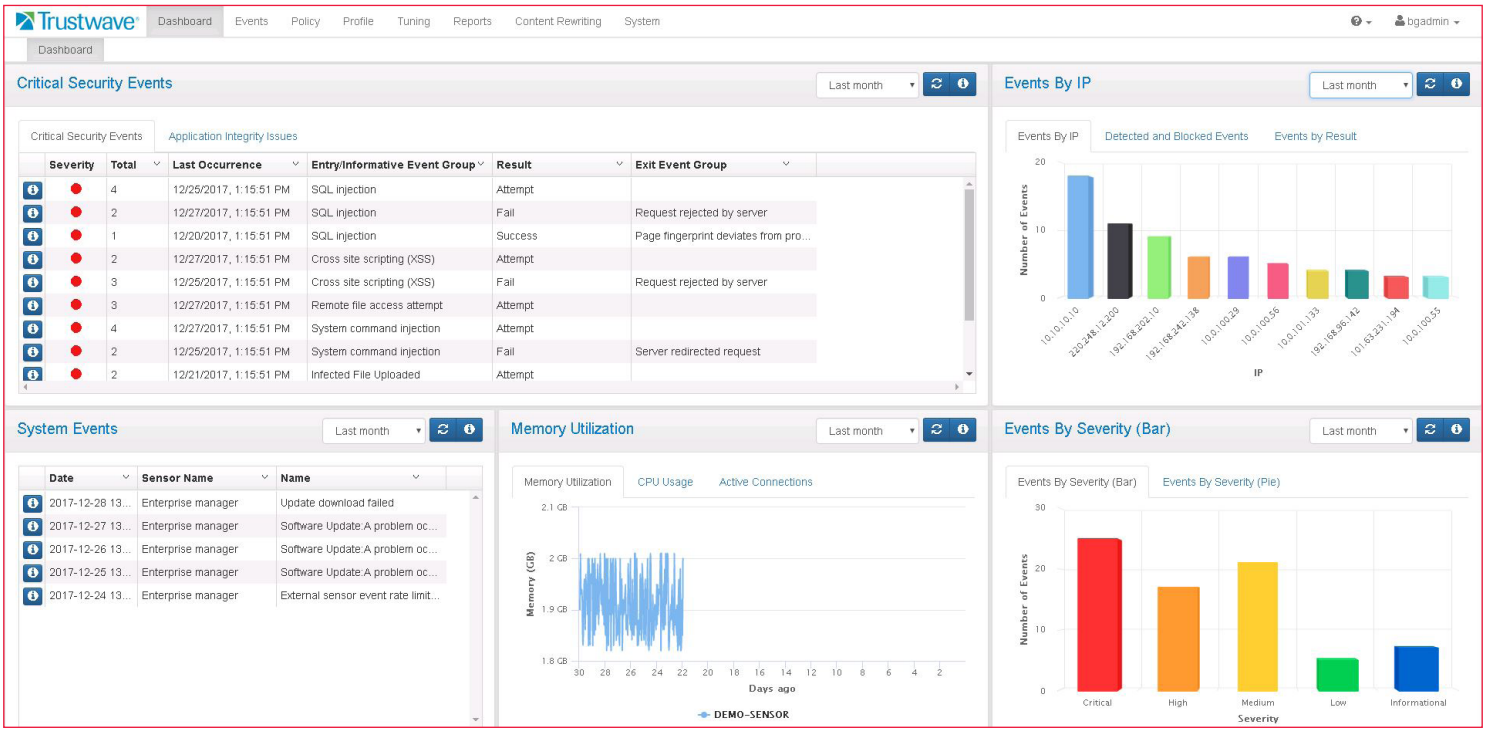
The Trustwave WAF helps you protect your valuable web applications and data by continuously monitoring traffic and enforcing policies to identify and block threats. Deploy and manage the Trustwave WAF yourself or have it managed by Trustwave security experts as a Managed WAF service.

Simplified Security

Attackers use a wide range of techniques to attack web applications: site scraping, malicious bots, zero-day, targeted attacks and more. The Trustwave WAF protects against these and others, including the OWASP Top 10 by offering a comprehensive set of capabilities, including:

- Positive Security: Real-time application profiling and misuse prevention
- Negative Security: Blocks known exploits
- User-Defined Rules: Customize scenarios for your unique applications
- Geo-Location: Block requests generated by specific countries
- Virtual Patching: Protect a vulnerable web application while developers are writing a fix
- Anti-Virus: Scan files for embedded viruses and malware before uploading to a web app
- Data Masking: Hide original data, like passwords, with random characters
- Rewrites: Conceal content, like internal codes, from external viewers

The Trustwave WAF is backed by the expertise of our elite SpiderLabs Research team who regularly update the WAF to detect new application vulnerabilities. The application layer signatures they create provide actionable information on detected vulnerabilities, so you get visibility into vulnerabilities and the details you need to quickly address them.



The intuitive and modern Trustwave WAF interface lets you easily view the status of your web applications, understand the context of events to quickly remediate issues, generate reports, and more.

Flexibility

There's no one way to deploy and use a WAF that works for every organization. That's why the Trustwave WAF offers multiple deployment and customization options. Implement it as a cloud service or deploy as a physical or virtual appliance. And depending on your needs, run it in- or out-of-line.*

Performance & Integrity

While a WAF is first and foremost a security control, the Trustwave WAF can also provide valuable application performance information that is useful for the development team, including programming mistakes, application errors or failures and insecure code.

The Trustwave WAF can also load balance incoming traffic across multiple backend servers. This reduces the risk of any one server becoming overloaded with requests and can eliminate the need for a separate load balancing solution.

Complementary Solutions & Services

In addition to the Trustwave WAF, Trustwave offers a complete portfolio of application security solutions to keep your applications—and your business—running in the face of persistent attacks. These include application and database scanning as well as application penetration testing. As you move from planning, building, testing, to running applications you can rely on Trustwave to provide protection every step of the way.

* Will vary by type of installation

Why Choose a Managed WAF?

Since vulnerabilities and web applications are always changing, an effective WAF should be tuned on a regular basis. You can do this yourself or have the WAF managed by Trustwave security experts. The Trustwave Managed WAF service includes:

- Deployment and tuning of the WAF appliance
- Continuous systems health monitoring
- 24x7x365 event monitoring and alerting, and periodic log review options
- Tuning support for scheduled changes to protected applications
- Access to events and reports through the MSS Portal
- Advanced web application security detection and protection

The Managed WAF service is delivered from Trustwave's worldwide SAS-70 compliant Security Operations Centers (SOCs). Skilled professionals in the SOCs augment you and your team by providing local coverage across various security disciplines and can assist other regions (or be assisted) as necessary so you get round the clock application security coverage.

Trustwave®

For more information: www.trustwave.com

WAF_0218