As organizations rely more and more on web applications to deliver services to their employees, partners, and customers, threats targeting websites are increasing rapidly because they are easy to exploit and have access to extremely valuable information.

Despite the vast resources available to help securely code web applications so they are less vulnerable to attack, known methods like SQL injection continue to be used in 80 percent of data breaches*. Also, even organizations that do perform dynamic application testing tend to do it infrequently due to the large number of web applications they have, the false positives, and sheer number of vulnerabilities that need to be addressed.

The reality is that web applications are a hacker’s favorite target and most organizations have trouble gaining actionable insight into the security of their websites.

Trend Micro Deep Security for Web Apps was developed to address today’s complex threat environment, providing a complete suite of security capabilities to find more critical vulnerabilities and provide actionable insight so you can protect against them.

* Verizon 2014 Data Breach Investigations Report

INTELLIGENT SECURITY FOR WEB APPLICATIONS

Complete Intelligent Application Scanning

...for today’s complex threat environment. Using both automatic scanning and human-augmented site audits, we cover more of the OWASP Top 10 critical web app risks and WASC testing criteria, while avoiding the false positives that bog down the security team.

Integrated Detection and Protection

...to minimize the time to respond to security threats. Quickly block new attacks with preconfigured WAF rules for leading vendors like Imperva, Citrix, ModSecurity, and AlertLogic.

Addressing Key Business Needs

Finds more critical vulnerabilities

With a combination of automated scanning and site audits by Trend Micro’s team of security experts, you’ll know if there are any OWASP Top 10 critical web app risks on your site.

Provides actionable insight into vulnerabilities

Detailed information is supplied, including proof of exploit, CVE ID, and potential solutions. Plus our security experts remove false positives from every scan.

Performs human-augmented site audits

Ensures you find logical flaws and vulnerabilities that can’t be found with automated scanning, such as broken authentication management, with periodic site audits by Trend Micro security experts. Includes comprehensive proof of exploitation.

Integrates with leading WAF vendors

Provides XML output for Web Application Firewalls (WAFs) that helps you quickly create new rules and block exploitation of vulnerabilities.

Eases compliance

Continuously scans applications to help you comply with regulatory requirements such as PCI DSS, HIPAA, etc.

Find out more at webappsecurity.TrendMicro.com
KEY FEATURES

Comprehensive Intelligent Application Testing

- Application vulnerability scanning that imitates user interaction to look for OWASP Top 10 web app risks and WASC testing criteria
- Comprehensive platform scanning (operating system and server) with over 50,000 checks to help you address PCI or other regulations
- Site audits by security experts to detect vulnerabilities that automatic scanning alone can’t catch
- Proof of exploit for critical vulnerabilities and expert vetting of scanning results to eliminate false positives
- Hidden malware detection with Trend Micro’s Smart Protection Network and specialized testing
- Monitoring of web application reputation to ensure there are no links to questionable or known infection vector websites
- AWS pre-authorized scanner so if you are hosting web applications in the cloud, you don’t need to request approval for scanning in advance

Find out more at webappsecurity.TrendMicro.com

Integrated Detection and Protection

- Based on discovered application vulnerabilities, quickly create Web App Firewall (WAF) rules to defend against application exploits before code and configuration fixes can be completed
- Support for rule export for WAF leaders like Citrix, Imperva, AlertLogic, and ModSecurity

Find out more at webappsecurity.TrendMicro.com
KEY FEATURES (continued)

Single Integrated Management Console

- All detection and protection functions are managed through a single cloud-based console with role-based administration to ease management of web app security
- Scanning can be done on-demand or can be run continuously to fit security needs
- Dashboard delivers information from both automatic and manual scanning, giving you a single view of your web application security posture
- Unlike other solutions, platform and application testing and results are consolidated in a single console
- Create custom or executive reports quickly

CLOUD-BASED AND SECURE

Provided as a service so there’s no installation or set up required, making it fast and easy to get up and running in minutes.

Pre-authorized scanner on AWS—so you don’t have to request advanced approval for scanning. Scan any web application hosted in AWS anytime, as often as you like.

No need to install product updates—malware patterns and infection vectors are automatically fed from our Smart Protection Network.

Native Integration with leading Web Application Firewalls

About Trend Micro

As a global leader in cloud security, Trend Micro develops security solutions that make the world safe for businesses and consumers to exchange digital information. With more than 25 years of experience, we deliver top-ranked security that fits our customers’ needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments.

Corporate member of

OWASP

The Open Web Application Security Project

GET STARTED!

See how easy it is to detect and protect your web applications with a free trial of Deep Security for Web Apps. Visit:

WEBAPPSECURITY.TRENDMICRO.COM

©2015 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. (030315Fv01a650g)