

Trend Micro™

Web Application Security

Safeguard your website against cyber attacks and data loss

Today's businesses rely on the availability of their revenue generating web applications to connect customers, suppliers, employees, and partners 24/7. Yet, website breaches are on the rise and compliance requirements for data security continue to develop. To secure your web presence and protect your business, you need to reduce your exposure by understanding your weaknesses. Trend Micro gives you immediate access to critical information that will help you prevent cybercriminals from exploiting vulnerabilities on your website.

Web Application Security helps you secure your websites before your systems are compromised by scanning them for vulnerabilities and generating detailed remediation reports. These reports prioritize activities so you can quickly correct weaknesses in your website's host- and application-layer security. Between scans, Web Application Security looks for evidence that your website has been hacked by constantly analyzing the Trend Micro Smart Protection Network. Should your website be identified as hosting malicious content, you will be immediately alerted so you can take action to prevent further damage to your corporate assets and reputation.

KEY FEATURES

Vulnerability Assessment

- Provides automated and manual scanning of your websites for web threats and vulnerabilities
- Automatically maintains the most current vulnerability libraries and remediation information
- Applies web-spidering technologies to scan multiple web applications, including the latest Web 2.0 applications
- Incorporates expert system and pass-through scanning methodologies to reduce false positives and probe deeper in vulnerabilities

Compliance Scanning (Coming Soon)

- Identifies vulnerabilities and associated risk across a wide range of web applications, databases, networks, operating systems, commercial applications and other software products
- Delivers accurate scanning results in less time, executing processes similar to that used by ethical hackers
- Promotes adherence to compliance issues like PCI, Sarbanes-Oxley, and HIPAA

Expert Reporting

- Provides summary and remediation reports, leveraging up-to-the-minute information from TrendLabsSM worldwide network of security experts
- Consolidates and prioritizes risk information into one centralized report, providing a

complete picture of security exposures so you can respond quickly

- Provides extensive information on vulnerabilities, in standardized reports that contain the right information, at the right level for your organization

Remediation Guidance

- Enables administrators to fix vulnerabilities quickly and easily with the information provided in remediation reports
- Helps you prioritize your IT security projects and minimize the time spent eliminating security vulnerabilities

Infiltration Monitoring & Alerting

- Provides continuous monitoring across the Trend Micro Smart Protection Network, looking for evidence that your websites' security has been compromised
- Alerts you immediately when your websites have been exploited and are hosting malicious content
- Enables you to quickly remediate your websites and mitigate the risk of harming your visitors or unwittingly distributing spam

Trustmark Service

- Provides optional SecureSite "trustmark" verification for public display to reinforce your ecommerce website's security certification
- Helps safeguard your ecommerce websites from hackers and malicious threats

HOSTED SCANNING SERVICE

Protection Points

- Web Applications
- Network Systems
- Hosted Operating Systems

Vulnerabilities Scanned

- Web 2.0 (JavaScript, AJAX, Flex)
- Cross-site Scripting
- SQL Injection
- Fraud/Phishing Enablers
- Unauthorized Use
- Outdated Host Patches

MONITORING SERVICE

- Powered by Smart Protection Network
- Malicious Content Identified
- Infiltration Alerts

KEY BENEFITS

- Reduces the time, risk, and cost of finding and fixing security vulnerabilities
- Addresses potential security issues before they impact your organization
- Helps assess and maintain strong data security by ensuring the security of web-facing systems and applications
- Eliminates the expense of purchasing and maintaining multiple products
- Simplifies deployment with software as a service provisioning
- Supports continuous 24/7 operations through a worldwide network of data centers

ELIMINATES COST OF PURCHASING AND MAINTAINING SECURITY SYSTEMS

As a web-based service, Web Application Security runs entirely from the Trend Micro in-the-cloud network. Vulnerability scans run on your schedule—automatically or manually—and the results are provided through a private web portal. The service requires no installation, no setup, no hardware purchases, no software development, no security expertise, and no special training or new technology to use. With our software as a service provisioning, all you have to do is enroll your company's domains and IP addresses and Trend Micro takes care of the rest. Trend Micro delivers the latest security vulnerability scanning and malware detection expertise, and our extensive knowledgebases are automatically updated with the latest information, reducing your exposure to a minimum.

SCANS	EXAMPLES	PROTECTS AGAINST
Application Layer	<p>Web Infrastructure—Apache, Apache Tomcat, Microsoft™ Internet Explorer, Mozilla FireFox, Microsoft™ IIS, FTP, BEA Weblogic, Adobe ColdFusion, SSH, TELNET, and shopping carts</p> <p>Web 2.0—JavaScript, AJAX, Adobe Flash applications</p> <p>Web Applications—Forms and contents residing on the website</p>	<ul style="list-style-type: none"> • Compromise of websites through cross-site scripting (XSS) vulnerabilities • Content spoofing • Javascript malware payloads • Vulnerabilities that can cause denial of services (DoS) on the website • Corruption or theft of data and identities
Databases	<ul style="list-style-type: none"> • Oracle • Microsoft™ SQL Server • Sybase • PostgreSQL • Sun™ MySQL • IBM™ DB2 • IBM™ DB2/400 • Lotus Notes™/Lotus™ Domino™ 	<ul style="list-style-type: none"> • SQL injection attacks designed to steal credit card data and identities • Configuration issues and policy compliance violations
Network Systems	Cisco™ firewalls, IPSec, PPTP, Network File System (NFS), DHCP, DNS, LDAP, SNMP	<ul style="list-style-type: none"> • System configuration issues, (eg. weak passwords) • Unauthorized access to systems
Operating Systems	Microsoft™ Windows™, Linux, UNIX, Sun™ Solaris™, Mac OS, BSC, IBM™ AIX™, IBM™ AS/400, Novell™ NetWare™	Access or compromise of OS from policy violations such as guessable passwords, file permissions, or inappropriate account access

SYSTEM REQUIREMENTS

To ensure proper operation of the web interface and to view reports, users of Web Application Security need an Internet connection and one of the following recommended browsers

- Microsoft Internet Explorer 6 or later
- Mozilla Firefox 1.5.x or later

EXTEND YOUR PROTECTION

- InterScan™ Web Security Virtual Appliance
- ServerProtect
- InterScan Messaging Hosted Service

WEBSITES BREACHES ON THE RISE

- Over 79% of websites hosting malicious code are legitimate—thus compromised by hackers (ZDNet, Apr 2008*)
- 50% of online retail sites have serious vulnerabilities (TrendLabs, 2008)
- More than 28,000 cross-site scripting vulnerabilities identified at named websites with only 5% fixed (www.xssed.com, Aug 2008)

* http://news.zdnet.com/2424-1009_22-198647.html

