

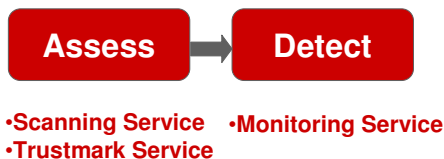
**Frequently Asked Questions:**

1. What is the Trend Micro Web Application Security solution?
2. Why do I need to protect my websites from attacks?
3. How can malware or hackers damage my website and business?
4. How do I know if Web Application Security is right for my business?
5. What is the SecureSite trustmark logo?
6. How does Trend Micro monitor whether my website has been hacked?
7. Can I evaluate Trend Micro Web Application Security?
8. How does your Web Application Security service work?
9. What types of website application components are scanned by Web Application Security?
10. How do I get the service configured to scan my Web servers?
11. Can Web Application Security work if I have a firewall?
12. Does Web Application Security scan my entire domain or just a portion of the website?
13. What are the vulnerabilities for which Web Application Security scans?
14. How long does a scan take?
15. How will the scans affect my Web servers?
16. What types of vulnerability reports are available?
17. Can users receive email notification of security scan results?
18. What report file formats can Web Application Security generate?
19. How is severity rated in the reports?
20. How does critical / severe / moderate map to CVSS?
21. What do the different severity levels in the vulnerability assessment reports mean?

**General**

**1. Question: What is the Trend Micro Web Application Security solution?**

**Answer:** The Trend Micro Web Application Security solution helps organizations secure their websites before systems are compromised, and continuously looks for evidence that their websites have been hacked so action can be taken to fix. It accomplishes this through a hosted service that provides the following functions:



Web Application Security dramatically reduces the time, risk and cost associated with securing a website by automatically scanning your websites for vulnerabilities and weaknesses across Web applications, networks, and host operating systems, and generating expert remediation reports through a hosted service. For qualifying ecommerce domains, an optional Trend Micro SecureSite trustmark logo can be displayed to reinforce your website’s security certification.

A monitoring service component of Web Application Security continuously checks the Trend Micro Smart Protection Network looking for evidence that your websites’ security has been compromised. Should your website be infiltrated, you are immediately alerted to the presence of malicious content.

And coming soon, the Advanced service will provide detailed compliance reports (addressing PCI, SOX, and HIPAA) which identify where policy violations exist, and the remediation actions required to come into compliance quickly.

Service Activities <i>- version 1.0</i>	Standard	Advanced <i>-Coming Soon</i>
Web application vulnerability scans	X	X
Host vulnerability scans	X	X

SecureSite trustmark service	X	X
Infiltration alerts	X	X
On-demand scans*	X	X
Reports	X	X
Compliance scans & reports (includes PCI, SOX, HIPAA)		X

\* 5 scans per year in Standard offering. Additional on-demand scans available as an add-on.

## 2. **Question:** Why do I need to protect my websites from attacks?

**Answer:** Websites are the open door to your business, providing a means for both visibility and revenue. However, many websites have vulnerabilities of which the business is not aware, yet expose their customer and data to potential attacks. To further complicate things, many times development and hosting of these websites are managed by third parties. Research shows that many websites are vulnerable:

- Over 79% of websites hosting malicious code are legitimate—thus compromised by hackers (ZDNet, Apr 2008)
- More than 28,000 known XSS vulnerabilities identified at named websites with only 5% fixed (source: XSSed.com, August 2008)
- More than 40% of Web threat incidents involved legitimate sites unknowingly distributing malware (source:TrendLabs, 2008)

## 3. **Question:** How can malware or hackers damage my website and business?

**Answer:** Hackers and online criminals make money by exploiting weaknesses in the Web, and stealing sensitive information, including credit card data. New attacks on Web and ecommerce sites are cropping up every day. It is time consuming and overwhelming for most businesses to understand the various threats such as Web2.0 exploits, SQL Injections, and other types of cross-site vulnerabilities. However, the burden of protecting sensitive information is the organization's responsibility, whether it is employee, customer, or business partner data. Security efforts to protect websites take focus away from developing the business, hence the vicious cycle. Losing the trust of these constituents diminishes your business reputation and puts revenue generating activities at risk. Indeed, many millions of consumers are simply afraid to use their credit cards online for fear of fraud and identity theft.

## 4. **Question:** How do I know if Web Application Security is right for my business?

**Answer:** Consider Web Application Security if you want to:

- Reduce the time, risk, and cost of finding and fixing security vulnerabilities in your websites.
- Find an easy and cost-effective means to assess and monitor the security posture of your websites.
- Have a trusted security expert help establish and maintain a more secure online experience for your prospects, customers, business partners, and employees.
- Develop strong data security practices and ensure the security of public-facing Web applications and systems.
- Address potential security issues before they impact your organization.
- Eliminate the expense of purchasing and maintaining multiple products.
- Simplify deployment with software as a service provisioning, requiring no additional hardware or software.

### 5. **Question:** What is the SecureSite trustmark logo?



**Answer:** The SecureSite trustmark logo Tested: 2 Sept, 2008 provides that third-party seal of approval to help your ecommerce customers understand that you have taken steps to protect their data. It is an optional service available with a daily scan that tests websites for vulnerabilities, dangerous content and links that expose consumers' computers and personal information to malicious use. Websites that meet security policies will be able to display the Trend Micro SecureSite trustmark on their Web pages to identify their security concern and diligence to Internet users. Web Application Security customers who choose a scan frequency other than "daily" will not be able to display the SecureSite trustmark logo on their site(s).

### 6. **Question:** How does Trend Micro monitor whether my website has been hacked?

**Answer:** The Trend Micro Smart Protection Network is a next-generation in-the-cloud content security infrastructure composed of a global network of sensors, with continuously updated and correlated threat databases which provide comprehensive protection against all types of threats—from malicious files, spam, phishing, and Web threats, to denial of service attacks, Web vulnerabilities, and even data loss. Web Application Security continuously monitors the Smart Protection Network looking for evidence that your websites' security has been compromised. And should one of your websites be infiltrated, you are immediately alerted via email to the presence of malicious content so you can take action and prevent further damage to your corporate assets and reputation. The monitoring process requires no dedicated scanning of your actual websites, but rather leverages the Smart Protection Network's real-time knowledge about threats on the Web. Additionally, if your site maintains a trusted or secure status, Trend Micro will periodically send you an email affirming this state just so you know we are working on your behalf.

### 7. **Question:** Can I evaluate Trend Micro Web Application Security?

**Answer:** Yes, the Web Application Security service is available to trial. The trial registration page is at:

<http://us.trendmicro.com/us/solutions/enterprise/security-solutions/web-application-security/trial>

To complete the registration, a publicly accessible domain or host IP address is required to be provided along with a valid email address. The opportunity to define the scan date and time allows you to schedule in accordance with your requirements. You will be emailed a confirmation upon submittal, and will be asked to post a small snippet of hidden text on your website to verify your ownership of that domain. Once your trial scan is complete, a follow-on email will be sent when your vulnerability scan report is ready for download. The confirmation will include the URL account and password information to access both your executive summary and remediation reports (note: for production customers, account password information will be communicated via the phone to ensure privacy). These reports will be available for 30 days on a private, secure Web portal for review. With the trial service, only one domain or IP address will be scanned for vulnerabilities; however the actual service supports organizations with 16 domains or more.

## Technical

### 8. **Question:** How does your Web Application Security solution work?

**Answer:** Since the Web Application Security vulnerability scans are a hosted, web-based service, it is quick and easy to start protecting your websites because there is no hardware or software to install. In addition, with hosted security managed by Trend Micro, you always have the latest technology and best protection.

- After you sign up, Web Application Security will scan your website per your schedule to assess weaknesses or vulnerabilities.
- After scanning, Web Application Security will assess the risk and deliver reports that you can quickly act upon to become more secure.
- The reports describe the safety status of your website including potential vulnerabilities, the severity of the issues, and recommended advice from experts on how to fix the issues. On-demand scans can be executed at your request to validate the success of your actions to remediate your website.
- If you choose to schedule daily scans, and pass our security criteria, you are eligible to display the SecureSite trustmark logo on your website, showing online customers that extra steps are taken to protect their online data and privacy.
- Web Application Security constantly monitors the Trend Micro Smart Protection Network looking for evidence that your websites' security has been compromised, and immediately alerts you to the detection of malicious content.

### 9. **Question:** What types of website application components are scanned by Web Application Security?

**Answer:**

Scans	Examples	Protects Against
Application Layer	<p><u>Web Infrastructure:</u> Apache, Apache Tomcat, Microsoft Internet Explorer, Mozilla Firefox, Microsoft IIS, FTP, BEA Weblogic, Adobe ColdFusion, SSH, TELNET, and shopping carts</p> <p><u>Web 2.0:</u> JavaScript, AJAX, Adobe Flash applications</p> <p><u>Web Pages:</u> Forms and content residing on the website</p>	<ul style="list-style-type: none"> <li>• Compromise of websites through cross-site scripting (XSS) vulnerabilities</li> <li>• Content spoofing</li> <li>• Javascript malware payloads</li> <li>• Vulnerabilities that can cause denial of services (DoS) on the website</li> <li>• Corruption or theft of data and identities</li> </ul>
Databases	<p>Oracle</p> <p>Microsoft SQL Server</p> <p>Sybase</p> <p>PostgreSQL</p> <p>Sun MySQL</p> <p>IBM DB2</p> <p>IBM DB2/400</p> <p>Lotus Notes/ Lotus Domino</p>	<ul style="list-style-type: none"> <li>• SQL injection attacks designed to steal credit card data and identities</li> <li>• Configuration issues and policy compliance violations</li> </ul>
Network Systems	<p>Cisco firewalls, IPSec, PPTP, Network File System (NFS), DHCP, DNS, LDAP, SNMP</p>	<ul style="list-style-type: none"> <li>• System configuration issues (e.g. weak passwords)</li> <li>• Unauthorized access to systems</li> </ul>

Operating Systems	Microsoft Windows, Linux, Unix, Sun Solaris, Mac OS, BSC, IBM AIX, IBM AS/400, Novell NetWare	<ul style="list-style-type: none"> <li>• Access or compromise of OS from policy violations, such as guessable passwords, file permissions, or inappropriate account access</li> </ul>
-------------------	---	---

**10. Question:** How do I get the service configured to scan my Web servers?

**Answer:** You will be sent a Web Application Security configuration form by our Operations Team on which you will record the domains and/or IP's you desire to have scanned for vulnerabilities and monitored for malicious content.

**11. Question:** Can Web Application Security work if I have a firewall?

**Answer:** Yes. It may be necessary for you to whitelist the Trend scanning server's IP address in your firewall/IDS/IPS to avoid inadvertently blocking the scan as a malicious attack.

**12. Question:** Does Web Application Security scan my entire domain or just a portion of the website?

**Answer:** The scan will follow the links to all pages on the website that are still listed as being under the domain requested. External links are not followed.

**13. Question:** What are the vulnerabilities for which Web Application Security scans?

**Answer:**

Fraud and Phishing Enablers	
<b>Cross-Site Scripting</b>	<b>Defrauds Users:</b> Most industry experts and researchers agree that cross-site scripting (XSS) continues to be the most prevalent website vulnerability. Depending on the website, XSS can be especially hazardous to businesses and consumers. New attack vectors employed are responsible for highly effective phishing scams and Web worms that are resistant to commonly accepted safeguards. The evolution of cutting-edge JavaScript malware as a payload has made finding and fixing this vulnerability more vital than ever.
Data Leaks	
<b>Information Leaks</b>	<b>Steals Proprietary Information:</b> Information leaks occurs when a website mistakenly reveals or is manipulated to reveal sensitive information such as developer comments, user information, internal IP addresses, source code, revision numbers, error messages/codes, etc..., which may all aid an attacker.
<b>Predictable URL</b>	<p><b>Uses Google Hacks:</b> Normally, the only mechanism protecting the sensitive information within is the predictability of the URL. Automated scanners have become adept at uncovering these files by generating thousands of guesses. In addition, through a process called "Google Hacking", attackers use search engines to discover sensitive information via forgotten links on a website.</p> <p><b>Finds Hidden Pages:</b> Over time, many pages on a website become unlinked, orphaned, and forgotten. These Web pages often contain payment logs, software backups, future press releases, debug messages, or source code.</p>

<b>SQL Injection</b>	<b>Steals Database Content:</b> SQL injection has been at the center of some of the largest credit card and identity theft incidents. Today's backend website databases store highly sensitive information, making them a natural, attractive target for malicious hackers. Names, addresses, phone numbers, passwords, birth dates, intellectual property, trade secrets, encryption keys and often much more could be vulnerable to theft. With a few well-placed quotes, semi-colons and SQL commands, entire databases could fall into the wrong hands.
<b>Directory Indexing</b>	<b>Finds Proprietary Pages:</b> As a feature of most popular Web servers, directory indexing lists the contents of a directory if no specific file name is given and no index file is present (example: index.html). Directory listings could reveal sensitive information not intended for public viewing, such as pre-released Web pages, log files, temporary files, backup files, etc...
<b>XPath Injection</b>	<b>Extracts Sensitive Data:</b> XPath Injection is an attack technique, similar to SQL Injection, used to exploit websites that construct XPath queries from user-supplied input. When an attacker is able to modify an XPath query, they may be able to obtain sensitive information from an XML document that would otherwise be out of reach.
<b>Unauthorized Use</b>	
<b>Insufficient Authentication</b>	<b>Allows Fraudulent Access:</b> Insufficient authentication flaws are typically found within the business logic of an application. Successful exploitation lets an attacker gain unauthorized access to protected sections of a website. For example, while logged-in as a normal user, an attacker could impersonate another user on the system.
<b>Abuse of Functionality</b>	<b>Uses Website Features Against User/Owner:</b> As stated by the Web Application Security Consortium Threat Classification, "Abuse of functionality is an attack technique that uses a website's own features and functionality to consume, defraud, or circumvent access controls mechanisms. Some functionality of a website, possibly even security features, may be abused to cause unexpected behavior. When a piece of functionality is open to abuse, an attacker could potentially annoy other users or perhaps defraud the system entirely."
<b>Buffer Overflow</b>	<b>Takes Control of Servers:</b> Exploits website vulnerabilities to take complete control of a server to perform malicious acts

#### 14. Question How long does a scan take?

**Answer:** The scan time is a function of the size of your website, the number of forms on the website, and the number of vulnerabilities detected on the website. Most scans for a single domain or IP address can be finished in less than 15 minutes. As a part of the first scanning cycle, Trend Micro will monitor the scan time for your domains and hosts so you can more efficiently schedule future scans.

#### 15. Question: How will the scans affect my Web servers?

**Answer:** Web Application Security does not employ scanning techniques known to cause disruption of network services. However, no network scanner can guarantee that scans will not produce side effects or disturbance of all systems. For example, scanning Web applications for cross-site scripting and SQL injection vulnerabilities requires the service to crawl every page of a target website, and submit the forms to analyze the server response. If you have any questions, please contact Trend Micro at [wfss\\_support@trendmicro.com](mailto:wfss_support@trendmicro.com).

#### 16. Question: What types of vulnerability reports are available?

**Answer:** Web Application Security provides both an Executive Summary and a Remediation Report.

- Executive Summary: Provides a high level overview of the security audit results, with summarized views and tables illustrating the state of your network and Web servers, including existing vulnerabilities by severity and category.

- **Remediation Report:** Delivers a detailed assessment, identifying the security risks that could adversely affect your critical Web operations and assets. In this report, the risks are quantified and an overall risk index is generated for each system allowing you to prioritize your remediation activities accordingly. For each host and vulnerability, a comprehensive remediation plan and set of recommended actions are defined, with the estimated time to resolve.

### 17. **Question:** Can users receive email notification of security scan results?

**Answer:** Yes, Web Application Security emails you upon the completion of each scan and subsequent posting of the reports to the Web portal. Additionally, should malicious content be hosted on your website and detected by the Trend Micro Smart Protection Network, you will be immediately alerted with details concerning the infected website and the malware present.

### 18. **Question:** What report file formats can Web Application Security generate?

**Answer:** Reports are posted in PDF format only for you to access via your account on our secure online Web portal.

### 19. **Question:** How is severity rated in the reports?

**Answer:** We use the CVSS (Common Vulnerability Scoring System) scoring system which assigned a 1-10 score for each vulnerability: <http://nvd.nist.gov/cvss.cfm>. We also map our 1-10 scale to the PCI scale to be able to create PCI reports. PCI reports will use the PCI severities and categories, which are often unrelated to what we may consider the severity (e.g., all denial of service = 3, all worms = 5, etc).

### 20. **Question:** How does critical / severe / moderate map to CVSS?

**Answer:**

- **Critical** - vulnerability on a system that is easily accessible, requires little or no authentication, and will provide the ability to; access confidential information, corrupt/delete data, or create a system outage. A score between 8 and 10 on the CVSS scoring system. Examples: No password on CIFS Administrator Account, Anonymous users can obtain the Windows password policy.
- **Severe** - vulnerability on a system that is accessible with a moderate level of experience, may or may not require authentication, and will provide; partial access to restricted information, access to destroy some information, and/or disable individual systems on a network. A score between 4 and 7 on the CVSS scoring system. Examples: Anonymous FTP Writeable, Weak LAN Manger hashing permitted.
- **Moderate** - vulnerability on a system that is accessible locally, requires authentication, and will provide; little or no access to unrestricted information, cannot destroy or corrupt information, and/or cannot cause outages on any systems. A score between 1 and 3 on the CVSS scoring system. Examples: Default or Guessable SNMP community names: public, OpenSSL PRNG Internal State Discovery Vulnerability.

### 21. **Question:** What do the different severity levels in the vulnerability assessment reports mean?

**Answer:** Critical vulnerabilities are those that are remotely exploitable, yield root or administrator access, or have an active worm or virus spreading in the wild. Severe vulnerabilities are those that are only locally exploitable; do not yield root access, or denial of service vulnerabilities. Moderate vulnerabilities are those that leak potentially sensitive information and could be used in conjunction with other vulnerabilities to launch an attack.