

GENERAL	1
1. What is Trend Micro™ SecureSite?	1
2. Why do I need to protect my website from attacks?	1
3. How do I know using SecureSite will make a difference to my online customers? ..	1
4. How do I know if SecureSite is right for my business?	2
5. How can malware or hacker damage my ecommerce site and business?	2
6. How does SecureSite work?	2
7. What type of damage do web threats cause to ecommerce sites?	2
8. I already use VeriSign in my ecommerce website. Why do I need SecureSite?	3
9. I already use a Privacy or Business Seal. Why do I need SecureSite?	3
TECHNICAL	3
10. Can SecureSite still work if I have a firewall?	3
11. Does SecureSite scan my entire domain or just a portion of the website?	3
12. What are the vulnerabilities for which SecureSite scans?	4

GENERAL

1. What is Trend Micro™ SecureSite?

Trend Micro™ SecureSite is a hosted, web-based solution for websites that enables online retailers or web hosting companies to automatically test websites for vulnerabilities via daily scanning and reporting. If vulnerabilities are found, online retailers can engage in-house IT resources or Trend Micro channel partners to remediate them using tips provided by TrendLab'sSM worldwide network of security experts. With this online service there is no additional hardware or software required to deploy, install, or maintain.

SecureSite service will test websites daily 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 a new Trend Micro SecureSite trust mark, as part of the service, to identify their security concern and diligence to Internet users..

2. Why do I need to protect my website from attacks?

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. Research shows that many websites are vulnerable:

- More than **28,000** known xss vulnerabilities identified at named websites with only 5% fixed (source: www.xssed.com, August 2008)
- More than **40%** of web threat incidents involved legitimate sites unknowingly distributing malware (source:TrendLabs, 2008)

3. How do I know using SecureSite will make a difference to my online customers?

As a small business, your website may not have the brand awareness of big business, so a third party seal of approval helps you customer understand that you have taken steps to protect their data.

- Over **70%** of online shoppers look for a third party seal of approval when they visit a website.(source: Opinion Reseach Study for IBM (<http://www-03.ibm.com/press/us/en/pressrelease/19154.wss>))

4. How do I know if SecureSite is right for my business?

Consider SecureSite if you want to:

- benefit from your significant investment in ecommerce business
- generate more revenue from your online business
- provide a safe and trusted shopping experience for your online shoppers
- find easy and cost-effective way to meet specific PCI DSS compliance regulations
- implement a highly secure and trusted solution requiring no additional hardware or software

5. How can malware or hacker damage my ecommerce site and business?

Hackers and online criminals make money by stealing sensitive information such as credit card numbers, personal and banking information, and more. As a result, ecommerce sites and the data that they can access are particularly attractive targets for the attackers.

New attacks on ecommerce sites are cropping up every day. It is time consuming and overwhelming for most businesses to understand the various threats such as Distributed Denial of Service (DDOS), SQL Injections, and other types of cross-site vulnerability or exploits from hackers or remote control bots. In addition, security efforts to protect ecommerce take focus away from developing business. There are many potential risks from online shopping, and they are well publicized. Indeed, many millions of consumers are simply afraid to use their credit cards online for fear of fraud and identity theft.

6. How does SecureSite work?

Since SecureSite is a hosted, web-based service, it is quick and easy to start protecting your ecommerce site 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, SecureSite will scan your ecommerce site each day to detect if it has identified weaknesses or vulnerabilities.
- After scanning, SecureSite 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 ecommerce site including potential vulnerabilities, the severity of the issues, and recommended advice from experts on how to fix the issues.
- Site owners who pass the daily scans or remediate vulnerabilities are eligible to display the SecureSite logo on their website,
- The SecureSite mark shows the website's online customers that extra steps are taken to protect the online customer data and privacy.

7. What type of damage do web threats cause to ecommerce sites?

By proactively detecting weaknesses and vulnerabilities, SecureSite is able to help prevent viruses, malware, spyware, and other malicious Web threats. The damage these Web threats can cause include:

- Loss of confidential information during on-line transactions
- Identify theft
- Denial of Service Attacks

8. I already use VeriSign in my ecommerce website. Why do I need SecureSite?

SecureSite is complimentary to VeriSign, augmenting your Verisign SSL security. Having SSL encryption wisely protects data in transit. Versign helps to confirm that the payment process itself is secured.

However, what about the security of the content, links, and images on your site that SSL does not address? Website vulnerability scanning, provided by SecureSite, helps defend your customers from malicious attacks and malware as well as protect your business and reputation.

VeriSign or other SSL Encryption	SecureSite
Offers strong SSL encryption that allows companies and their customers to exchange information securely.	Provides vulnerability scanning of the website to identify weaknesses and provide tips on how to fix vulnerabilities.

9. I already use a Privacy or Business Seal. Why do I need SecureSite?

SecureSite is complimentary to Privacy and Business Seals.

- **Privacy Seals** help to verify that a company has certain statements in their privacy policy protecting their customer data.
- **Business Seals** focuses on helping to confirm that the company is a real entity by confirming the company is who they say they are.
- **SecureSite** is complimentary to these by performing a daily scan of a site, checking for vulnerabilities to protect consumers from crimeware, phishing and other web threats.

TECHNICAL

10. Can SecureSite still work if I have a firewall?

Yes, however, for first time use of SecureSite, it is required to open certain ports and include the specific IP address in the allowed list. Refer to the technical documentation for more detailed information.

11. Does SecureSite scan my entire domain or just a portion of the website?

SecureSite identifies security weaknesses in many layers of a network computing environment and provides vulnerability information, risk assessment, and remediation information.

12. What are the vulnerabilities for which SecureSite scans?

Fraud and Phishing Enablers	
Cross-Site Scripting	Defrauds Users: 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	
Information Leaks	Steals Proprietary Information: 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.
Predictable URL	Finds Hidden Pages: 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. Uses Google Hacks: 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.
SQL Injection	Steals Database Content: 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 command entire databases could fall into the wrong hands.
Directory Indexing	Finds Proprietary Pages: 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...
XPath Injection	Extracts Sensitive Data: 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.
Unauthorized Use	
Insufficient Authentication	Allows Fraudulent Access: 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.
Abuse of Functionality	Uses Website Features Against User/Owner: 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.”
Buffer Overflow	Takes Control of Servers: Exploits website vulnerabilities to take complete control of a server to perform malicious acts