

Introduction

On April 7, 2008, Trend Micro released **Trend Micro™ Web Protection Add-On**. This document is intended to answer the most frequently asked questions about this new technology.

Overview

Trend Micro Web Protection Add-On is a lightweight client that complements existing antivirus solutions by providing a glimpse of some of Trend's leading-edge technologies, namely Trend Micro Web Threat Protection and "in-the-cloud" bot behavior analysis capabilities.

Trend Micro Web Threat Protection monitors outbound Web requests to protect your PC against malicious threats hosted on infiltrated or specially crafted Web sites. In-the-cloud bot behavior analysis capabilities monitor your computer for suspicious behavior associated with bots, a form of malicious software that can secretly take control of your computer for criminal purposes.

Trend Micro Web Protection Add-On is highly proactive, because it is designed to intercept malicious threats at the earliest possible point of infection—"in the cloud," before they reach and infect the endpoint." By intercepting malware "in the cloud," the need for resource-intensive threat scanning and clean-up on the endpoint itself is greatly reduced.

In addition, Trend Micro Web Threat Protection technology is designed to block access attempts to potentially malicious Web sites in real time. If evidence of potential bot infection is detected, Trend Micro Web Protection Add-On will direct you to **Trend Micro™ HouseCall™** for a full system scan and clean.

Frequently Asked Questions

Q1. Where can I download Trend Micro Web Protection Add-On?

A: Customers and partners interested in evaluating the power of Trend Micro's Web Threat Protection technology may download Trend Micro Web Protection Add-On from Trend Micro's Web site at www.trendmicro.com/go/WebThreatChallenge.

Q2. Will Trend Micro Web Protection Add-On time out?

A: Yes. Trend Micro Web Protection Add-On is a trial designed to demonstrate the power of Trend Micro's Web Threat Protection technology. Trend Micro Web Protection Add-On will time out after a period of 90 days from installation.

Q3. What happens when the 90-day time-out period expires?

A: The main console will display a service expired message when the 90-day time-out period expires, and the trial will no longer perform its functions. You will be directed to Trend Micro's Web site for information on how [Trend Micro Enterprise and SMB products](#) can help protect you against Web threats.

Q4. What is Trend Micro Web Protection Add-On?

A: Trend Micro Web Protection Add-On is a lightweight client trial that complements existing antivirus solutions by providing a glimpse of some of Trend's leading-edge technologies, namely Trend Micro Web Threat Protection and "in-the-cloud" bot behavior analysis capabilities.

Trend Micro Web Threat Protection monitors outbound Web requests to protect your PC against malicious threats hosted on infiltrated or specially crafted Web sites. Its in-the-cloud bot behavior analysis

capabilities monitor your computer for suspicious behavior associated with bots, a form of malicious software that can secretly take control of your computer for criminal purposes.

Trend Micro Web Protection Add-On is highly proactive, because it is designed to intercept malicious threats at the earliest possible point of infection—"in the cloud," before they reach and infect the endpoint." By intercepting malware "in the cloud," the need for resource-intensive threat scanning and clean-up on the endpoint itself is greatly reduced.

In addition, Trend Micro Web Threat Protection technology is designed to block access attempts to potentially malicious Web sites in real time. If evidence of potential bot infection is detected, Trend Micro Web Protection Add-On will direct the user to Trend Micro HouseCall for a full system scan and clean.

Q5. What is the definition of "in-the-cloud" as it relates to Trend Micro Web Protection Add-On?

A: "In-the-cloud" refers to an entity that exists on the Internet network. Traditional endpoint-based malware behavior analysis performs analysis operations on the endpoint using sets of analysis rules stored locally on the endpoint. Trend Micro Web Protection Add-On is revolutionary because these rules exist "in the cloud" and the actual analysis occurs "in the cloud," before a threat reaches the endpoint. This reduces the need for frequent rule updates on the endpoint as well as the "time-to-protection" against the latest threats.

Q6. What is the definition of a "known threat" as it relates to Trend Micro Web Protection Add-On?

A: By the traditional method of "blacklist-only," signature-based classification, a threat is said to be known because it has undergone analysis at a threat research lab. Conversely, an unknown threat has not undergone this type of analysis.

Q7. What is the definition of a "bot" as it relates to Trend Micro Web Protection Add-On?

A: A bot (short for "robot") is a program that operates as an agent for a user or another program or simulates a human activity. On the Internet, the most ubiquitous bots are the programs (also called spiders or crawlers) that access Web sites and gather their content for search engine indexes.

Q8. Does Trend Micro Web Protection Add-On have any installation or operating system requirements?

A: Trend Micro Web Protection Add-On can protect computers meeting the following operating system and hardware requirements:

Supported operating systems:

- Microsoft™ Windows™ 2000 Professional Edition (with the latest Service Pack)
- Microsoft Windows XP Professional Edition (with the latest Service Pack)
- Microsoft Windows XP Home Edition (with the latest Service Pack)
- Microsoft Windows Server™ 2003 Enterprise Edition (with the latest Service Pack)
- Microsoft Windows Server 2008 Enterprise (with the latest Service Pack)
- Microsoft Windows Vista™ (32-bit version only) (with the latest Service Pack)

Hardware requirements:

- Intel™ Pentium™ 350MHz and above
- Windows Vista needs at least Intel Pentium 800MHz
- At least 128MB RAM
- Windows Vista needs at least 512MB RAM
- At least 250MB free disk space
- IPv4 Internet connection

Q9. Is Trend Micro Web Protection Add-On available in languages other than English?

A: At this time, Trend Micro Web Protection Add-On is available in English only. In addition, please note that at this time, Trend Micro Web Protection Add-On has only been tested on the U.S. English language versions of the supported operating systems.

Q10. Will Trend Micro Web Protection Add-On technology be added to other Trend Micro products or offered as a standalone solution?

A: Trend Micro Web Threat Protection technology is already available in a number of Trend Micro solutions, including the following:

- Trend Micro OfficeScan™ 8.0 ([Details](#))
- Trend Micro Internet Security 2008 ([Details](#))
- Trend Micro Internet Security Pro ([Details](#))
- Trend Micro InterScan™ Gateway Security Appliance ([Details](#))
- Trend Micro InterScan Messaging Hosted Security ([Details](#))
- Trend Micro InterScan Messaging Security Appliance ([Details](#))
- Trend Micro InterScan Messaging Security Suite ([Details](#))
- Trend Micro InterScan Web Security Appliance ([Details](#))
- Trend Micro InterScan Web Security Suite ([Details](#))
- Trend Micro HouseCall ([Details](#))
- Trend Micro TrendProtect™ ([Details](#))

There are currently no plans to make Trend Micro Web Protection Add-On available as a standalone product. Trend Micro Web Protection Add-On is a trial designed to demonstrate the power of Trend Micro's Web Threat Protection technology included in current and future Trend Micro solutions.

Trend Micro research and development teams are constantly working to investigate, prototype and test new technologies in our continuous efforts to protect our customers against the most prevalent threats. Future integration and release plans for Trend Micro Web Protection Add-On technology and other new technologies will be communicated to our customers and partners at the time of future product releases.

Q11. What do I need to know about Trend Micro Web Protection Add-On compatibility with other security software?

A: Since Trend Micro Web Protection Add-On is not intended to be a total protection solution, Trend Micro conducted compatibility testing with the most commonly used security solutions as part of the beta program for Trend Micro Web Protection Add-On. For information on supported and incompatible products, please refer to the Readme.txt file.

Q12. What happens if I install Trend Micro Web Protection Add-On on a system running a security solution for which Trend Micro has not done any compatibility certification?

A: We will not prevent installation of Trend Micro Web Protection Add-On on a system running a competing solution for which we have not done any compatibility certification. In instances where we determined during our testing that Trend Micro Web Protection Add-On is not compatible with a competing solution, we employ checks to ensure that Trend Micro Web Protection Add-On can't be installed alongside this competing solution. For a list of incompatible solutions, please refer to the Readme.txt file.

Q13. What happens if the user experiences incompatibility issues with other security products Trend Micro has not certified against after installing Trend Micro Web Protection Add-On?

A: In cases where the user experience is adversely affected due to an unforeseen incompatibility, we would appreciate your feedback. On the main Trend Micro Web Protection Add-On screen, click on "Settings" and then select the "Feedback" button. We will do our best to incorporate feedback into updates of the technology. In the meantime, we suggest uninstalling Trend Micro Web Protection Add-On in the event your user experience is adversely affected.

Q14. Will running Trend Micro Web Protection Add-On on a computer impact performance?

A: Trend Micro Web Protection Add-On has a very small installer CPU and memory footprint. Because there is no pattern required, the resource utilization of the application is minimized.

Q15. What do I need to do after installing Trend Micro Web Protection Add-On?

A: Nothing. Trend Micro Web Protection Add-On works in the background, checking for Web threats and signs of bots on your computer. If Trend Micro Web Protection Add-On notices any suspicious behavior associated with Web threats or bots, it will alert you.

Q16. How do I use Trend Micro Web Protection Add-On?

A: To use Trend Micro Web Protection Add-On, just make sure that your computer has a working Internet connection. If your computer connects to the Internet through a home network, Trend Micro Web Protection Add-On can use your current network settings automatically. If your computer connects to the Internet through a proxy server, then you must specify the server settings by clicking “Settings” on the main screen of Trend Micro Web Protection Add-On.

Q17. How do I remove Web threats or bots?

A: If a Web threat or bot infects your computer, the Trend Micro Web Protection Add-On system tray icon changes to alert you. Because bots are typically computer worms (a type of malicious software that can propagate from one computer to another), you must scan and clean your computer using an effective antivirus program to remove a bot. If you have an antivirus program installed, download the latest security update and scan your computer. To scan and clean your computer for free, visit [Trend Micro HouseCall](#) online.

Q18. Does Trend Micro Web Protection Add-On detect anything other than Web threats or bots?

A: The focus of Trend Micro Web Protection Add-On is on the detection of Web threats and bot behavior, which make up the vast majority of threats today.

Q19. What are Web threats?

A: Any threat that uses the Web to do malicious and unwanted things; characteristics include:

- Use the Web to perform malicious and often self-perpetuating activities
- Typically consist of one or more malicious programs that are installed on a user's computer without his/her knowledge, permission or understanding when the user accesses the Internet
- May either be invisible or seem benign to the user, but when activated individually or in combination can steal confidential information from the user's computer or use the computer's resources without the user's knowledge or permission

Q20. What are some examples of Web threats?

A: The following are examples of Web threats:

- Spyware installed upon visiting a Web site
- A bot that receives commands via IRC or through Web pages
- Adware installed after downloading a cool program from the Internet
- A Trojan installed from a JPEG exploit upon visiting a Web site that was clicked from an email received
- A virus, spread from a program downloaded from the Internet
- A worm that started blasting copies of itself, after disguising itself as a downloadable widget for golfers

Q21. Web threats aren't new. What's changed?

A: Web threats are more pervasive today and are the fastest growing threat vector. They are much more sophisticated, comprised of multiple components, and leverage the Web to update, hide, communicate, and transmit stolen information. Growing numbers of people worldwide are going online, and the Web has become an intrinsic part of their lives. With hackers becoming more organized and increasingly motivated by profit, criminal opportunity is greater than ever, threatening users with the loss of intellectual property or private data.

Q22. Why do I need to be concerned about Web threats more than ever before?

A: Motivated by the lure of profits from the sale of stolen confidential information, malware writers today are shifting to the Web as the medium of their malicious activities. Characterized by blended techniques, an explosion of variants, and targeted and regional attacks, Web threats pose a broad range of potential costs, including identity theft, loss of confidential corporate information, damaged brand reputation, and loss of consumer confidence in Web commerce. These high stakes, the pervasive use of the Web, and the complexity of protecting against Web threats combine to form perhaps the greatest challenge to protecting the privacy of personal information and the confidentiality of corporate information in a decade.

Q23. Why don't traditional protection methods protect against Web threats?

Traditional means do not provide adequate protection from these threats, and no single method or technology will improve this situation. Instead, a multi-layered, comprehensive solution must be brought to bear to address this fast growing class of threats.

Q24. What are the benefits of Trend Micro's Web threat protection solutions?

Trend Micro's Web threat protection solutions offer a multi-layered, multi-threat approach to dealing with Web threats, including innovative technologies deployed at the gateway, in the network, on the PC, and "in the cloud." These technologies work seamlessly together to proactively respond to new and emerging Web threats. Trend Micro's Web threat protection solutions provide a unifying vision to existing and impending products and services from consumer, SMB, and enterprise segments. With this vision, Trend Micro demonstrates a depth of understanding of current and emerging threats and technological innovation to create best-in-class solutions.

Q25. Do I need Trend Micro Web Protection Add-On?

A: Security experts believe that millions of computers have already become infected with Web threats and bots without the knowledge of their owners. Even if no Web threats or bots currently lurk on your computer, installing Trend Micro Web Protection Add-On can reduce the risk of your becoming a victim.

Q26. Don't Trend Micro's current desktop products already detect Web threats and bots?

A: Yes, Trend Micro's current products do detect Web threats and bot code that are installed on an infected computer. Trend Micro Web Protection Add-On is a tool primarily designed to demonstrate the power of Trend Micro's Web Threat Protection technology to new customers. For a list of Trend Micro solutions that already include Trend Micro Web Threat Protection technology, please refer to [Q10](#) above. Note also that products currently available use signature-based bot technology. Trend Micro Web Protection Add-On is using new dedicated, event-based behavioral technology that does not require signatures and detects bot activity in real time. This means that Trend Micro Web Protection Add-On has a reduced need for regular updates and consumes fewer resources on the user's computer. Updates are managed by Trend Micro "in the cloud," which means the application is always up-to-date.

Q27. How do I get technical support for Trend Micro Web Protection Add-On?

A: Although Trend Micro does not provide free technical support for Trend Micro Web Protection Add-On, we welcome your [feedback](#). On the main Trend Micro Web Protection Add-On screen, click on "Settings" and then select the "Feedback" button. You may also submit your feedback directly via Trend Micro's [Web site](#). We will do our best to incorporate feedback into updates of the technology.

©2008 Trend Micro Incorporated. All rights reserved. The information contained in this document represents the information available to Trend Micro at the time of publication and is provided "AS IS," without warranty of any kind. This document is subject to change without notice. Trend Micro, the Trend Micro t-ball logo, HouseCall, InterScan, OfficeScan and TrendProtect are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

