

Trend Micro™

Patch Management Module for Endpoint Security Platform

Reinforce your security with instant, complete, scalable patch management

Escalating exposure to sophisticated malware has left endpoints the most at-risk point in the network. But using anti-malware software alone only addresses a symptom of the problem instead of getting to the root of the disease—patching vulnerabilities. However, it is difficult to effectively monitor, patch, and update machines in distributed, heterogeneous environments. Software vendors, such as Microsoft, provide some patch management capabilities, but this is limited to the vendor's operating system or software. Vulnerability research conducted in 2008 shows that many popular applications went unpatched, ranging from 24% for Adobe Reader to 96% for Sun Java JRE. This included 44% of all Word 2003 installations.¹ This inefficient approach to patch management creates a gap in security, drains resources, reduces productivity, and increases enterprise risks and costs.

Even when enterprises attempt to patch vulnerabilities, poor visibility and limited reporting make it difficult to determine whether patches have been successfully installed or why a given fix failed to execute. And the larger the organization, the more extensive the patch management challenges can become, requiring a substantial number of staff to oversee the work.

In large, geographically distributed organizations, network bandwidth limitations can make patching a slow and cumbersome process, consuming a significant amount of limited network bandwidth—sometimes up to 90 percent. This can essentially shut out access to critical business applications, disrupt productivity, and create user dissatisfaction, especially if users are forced to accept an update at the moment it is delivered—often with a mandatory reboot. Finally, many solutions do not allow administrators to deploy a patch or update when a computer is off the network, which has become increasingly problematic with the growth in mobile workers.

GET IMMEDIATE PROTECTION ON EVERY ENDPOINT

Trend Micro Patch Management Module overcomes the obstacles to ensuring updated patches on every endpoint through its distributed intelligence, broad platform coverage, bandwidth throttling capabilities, and unparalleled insight into the patch management process. As part of the Endpoint Security Platform, Patch Management Module leverages a single console to centrally control and process patches for a variety of software vendors—all on a single server that can scale to support over 250,000 endpoints, regardless of their location, connection type, or status. In addition, bandwidth throttling capabilities ensure no loss of functionality over low-bandwidth or globally-distributed networks, increasing first-pass patch installation success rates to ensure that machines have actually implemented the received patch.

Patch Management Module provides the instant visibility needed to ensure up-to-date protection, providing real-time reports on which patches were deployed, on which endpoints, when they were sent, and who deployed them. When combined with other Endpoint Security Platform modules, enterprises are able to view both anti-malware and patch management status together in the same console, providing more effective endpoint protection and saving time, effort, and cost through system consolidation. Patch Management Module helps organizations meet their service level agreements as well as regulatory and internal compliance requirements in a solution that is faster, more successful, and more cost-effective than any other system.

PLATFORM MODULE

Solution Platform

- Trend Micro Endpoint Security Platform

Available Modules

- Patch Management Module
- Core Protection Module
- Web Protection Module
- Data Leak Prevention Module

KEY BENEFITS

- Covers fixed and mobile computers, both within and outside of enterprise firewalls
- Reduces patch and update times from weeks and days to hours and minutes
- Increases first-pass success rates from 60-75% to 95-99+%
- Lowers the workload of system administrator by 75% or more
- Scales to manage over 250,000 endpoints from a single server
- Assures compliance with internal and external standards and requirements

¹ Secunia: Stay Secure, 2008 Report

TREND MICRO SIMPLIFIES PATCH MANAGEMENT

Trend Micro Patch Management Module for Endpoint Security Platform centralizes control and processes. Six key patch management steps are automated using a highly flexible approach, considerably reducing staffing and time requirements.

- 1. Research.** The Patch Management Module frees customers from having to research new patches by publishing information from software vendors' patch bulletins and providing it in a policy content stream.
- 2. Assess.** When new patch information is available, each Endpoint Security Platform Agent automatically assesses each endpoint against the patch policy definition to determine if installation is necessary. The Agents then notify the Endpoint Security Platform Server if the patch is needed.
- 3. Remediate.** Endpoint Security Platform management console enables system administrators to instantly review, prioritize, and deploy patches whenever needed.
- 4. Confirm.** The Endpoint Security Platform Agent verifies that the patch has been successfully applied and reports status back to the management console.
- 5. Monitor.** The Endpoint Security Platform Agent continually monitors endpoints to ensure that they remain updated, reapplying the required patch should any endpoint fall out of compliance.
- 6. Report.** The Endpoint Security Platform's integrated web reporting capability allows end users, executives, management, and others to get updated reports in real time.

KEY FEATURES

Complete Coverage

- Enables centralized delivery of software patch management and security updates for major operating systems and common commercially-available applications
- Allows the deployment of custom patches
- Enables groups of patches to be deployed as a single entity based on criteria set by the administrator
- Detects and remediates corrupt patches

Instant Access

- Covers fixed and mobile computers, both within and outside of enterprise firewalls
- Ensures no loss of functionality over low-bandwidth or globally-distributed networks, increasing first-pass patch installation success rates from 60-75% to 95-99%
- Automates self-assessment analysis conducted on endpoints—no centralized or remote scanning server required

Pervasive Visibility

- Uses a lightweight agent to continually monitor the status of updated machines
- Offers real-time visibility to ensure up-to-date protection with detailed patch deployment and installation reports

Scalable Protection

- Requires minimal hardware and license requirements, generally just a single server
- Scales to support 250,000 endpoints from a single management server
- Reduces patch and update times from weeks and days to just hours and minutes, using intelligent relays that provide targeted patch installation only where needed

SYSTEMS REQUIREMENTS

For the Endpoint Security Platform

Supported Operating Systems for Management Server

- Windows 2000 Server SP 2+/2003/2008

Database Requirements for Management Server

- SQL Server 2000 SP4/2005

Supported Operating Systems for Management Console

- Windows XP/2000/2003 Vista/2008

SUPPORTED OPERATING SYSTEMS

For Patch Management Module

- Windows
- Mac OS X
- Sun Solaris
- IBM AIX
- IBM zLinux
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Red Hat Linux

Note: Functionality may vary by supported platform. For an updated listing of supported operating systems, please contact your Trend Micro representative.



©2009 by Trend Micro Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo 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. [DS01_ESP_PatchMgt_090403US]

www.trendmicro.com