IBM Tivoli Endpoint Manager for Patch Management

Continuous patch compliance visibility and enforcement

Highlights

- Automatically manage patches for multiple operating systems and applications across hundreds of thousands of endpoints regardless of location, connection type or status
- Reduce security and compliance risk by slashing remediation cycles from weeks to days or hours
- Gain greater visibility into patch compliance with flexible, real-time monitoring and reporting
- Provide up-to-date visibility and control from a single management console

With software and the threats against that software constantly evolving, organizations need an effective way to assess, deploy and manage a constant flow of patches for the myriad operating systems and applications in their heterogeneous environments. For system administrators responsible for potentially tens or hundreds of thousands of endpoints running various operating systems and software applications, patch management can easily overwhelm already strained budgets and staff. IBM Tivoli® Endpoint Manager for Patch Management balances the need for fast deployment and high availability with an automated, simplified patching process that is administered from a single console.

Tivoli Endpoint Manager for Patch Management, built on BigFix® technology, gives organizations access to comprehensive capabilities for delivering patches for Microsoft® Windows®, UNIX®, Linux® and Mac operating systems, third-party applications from vendors including Adobe®, Mozilla, Apple and Java™, and customer-supplied patches to endpoints—regardless of their location, connection type or status. Endpoints can include servers, laptops, desktops, and specialized equipment such as point-of-sale (POS) devices, ATMs, and self-service kiosks.

Apply only the correct patches to the correct endpoint

One approach to patch management is to create large patch files with a large update "payload" and distribute them to all of the endpoints, regardless of whether they already have all of the patches or not.

Tivoli Endpoint Manager for Patch Management takes a different approach, automatically creating patch policies, called IBM Fixlet® messages, which wrap the update with policy information such as patch dependencies, applicable systems, and severity level. An intelligent endpoint agent recognizes which patches are required for the machine that it is installed on, based on the endpoint's unique hardware, operating system, configuration settings, applications and patches already installed. The agent then automatically retrieves and applies only the relevant updates that are needed for that specific endpoint.

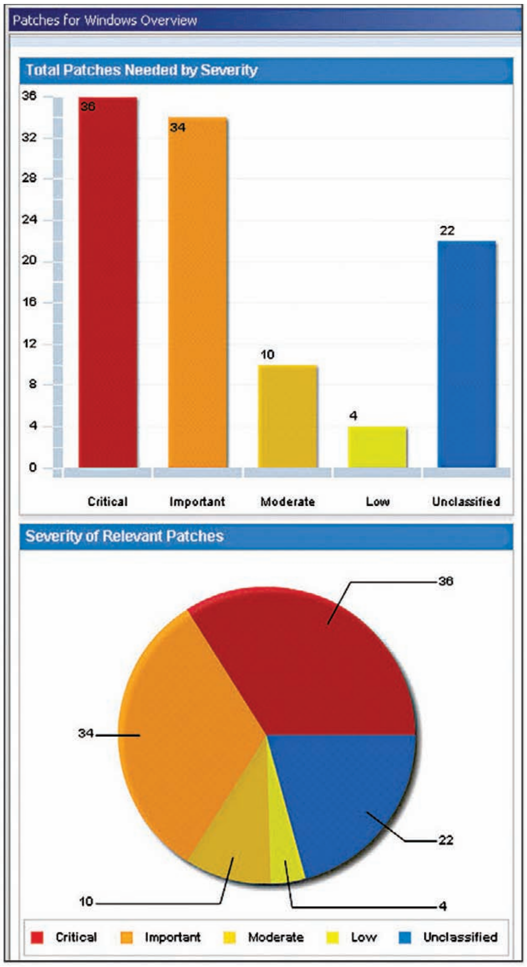
Accelerating and automating the patch management process

Tivoli Endpoint Manager for Patch Management automates the entire patch management process and enhances security while saving money, time and effort.

Research—Tivoli Endpoint Manager acquires, tests, packages and distributes many patch policies directly for customers, removing considerable patch management overhead. This largely automated process provides a consistent, high-quality patch in a timely manner.

Assess—The Tivoli Endpoint Manager intelligent agent continuously monitors and reports endpoint state, including patch levels, to a management server. This intelligent agent also compares endpoint compliance against defined policies, such as mandatory patch levels.

Remediate—Organizations can quickly create a report showing which endpoints need updates and then distribute those updates to the endpoints within minutes. IT administrators can safely and rapidly patch Windows, Linux, UNIX, and Mac operating systems with no domain-specific knowledge or expertise, and the solution stores audit information that tracks who ordered which updates to be applied to which endpoints.



Tivoli Endpoint Manager for Patch Management dashboards and reports show patch management progress in real time.

Confirm—Once a patch is deployed, Tivoli Endpoint Manager automatically reassesses the endpoint status to confirm successful installation and immediately updates the management server in real time. This step is critical in supporting compliance requirements, which require definitive proof of patch installation. With this solution, operators can watch the patch deployment process in real time via a centralized management console to receive installation confirmation within minutes of initiating the patch process. By closing the loop on patch times, organizations can ensure patch compliance in a way that is smarter and faster.

Enforce—The intelligent agent provides continuous endpoint enforcement and ensures that endpoints remain updated. If a patch is uninstalled for any reason, the agent can be configured to automatically reapply it to the endpoint as needed.

Report—Integrated web reporting capabilities allow end users, administrators, executives, management and others to view dashboards and receive up-to-the-minute reports. Dashboards and reports indicate which patches were deployed, when they were deployed, who deployed them, and to which endpoints. Special "click through" dashboards show patch management progress in real time.

Continuous compliance

Many organizations need to establish, document and prove compliance with patch management processes in order to comply with governmental regulations, service level agreements (SLAs) with other organizations and internal constituents, and corporate policies. Regulations such as Sarbanes-Oxley, PCI DSS and HIPAA require that a regular, fully documented patch management process be in place, and proof of continuous compliance is necessary in order to pass audits. This solution's ability to enforce policies and quickly report on compliance can help improve an organization's audit readiness.

Simple to use, yet vast in scope

A single patch management server can support up to 250,000 endpoints, shortening patch times and updates with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks. The solution features patented bandwidth throttling technology that manages network traffic and minimizes congestion.

Customers have achieved 95+ percent first pass success rates—up from the conventional 60 to 75 percent rate—not only increasing the effectiveness of the patch process but cutting operational costs and reducing staff workloads by as much as 20:1. The solution can patch endpoints on or off the network—including devices using Internet connections—with minimal endpoint impact. This means laptops using a public Internet connection at a coffee shop and other "roaming" devices can still receive patches.

Tivoli Endpoint Manager family at a glance

Server requirements:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

Console requirements:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

Supported platforms for the agent:

- Microsoft Windows, including XP, 2000, 2003, Vista, 2008, 2008 R2, 7, CE, Mobile, XP Embedded and Embedded Point-of-Sale
- Mac OS X
- Solaris
- IBM AIX®
- Linux on IBM System z®
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Oracle Enterprise Linux
- CentOS Linux
- Debian Linux
- Ubuntu Linux

For more information

To learn more about IBM Tivoli Endpoint Manager for Patch Management, contact your IBM sales representative or IBM Business Partner, or visit: **ibm.com**/tivoli/endpoint

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT life cycle management, and is backed by world-class IBM services, support and research.

The information provided in this document is distributed "as is" without any warranty, either express or implied. IBM expressly disclaims any warranties of merchantability, fitness for a particular purpose or noninfringement. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

Tivoli® software

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
February 2011

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Please Recycle