

IBM Tivoli Endpoint Manager for Security and Compliance

A single solution for managing endpoint security across the organization



Highlights

- Provide up-to-date visibility and control from a single management console
 - Employ a single, multipurpose, intelligent agent that assesses and remediates issues to help ensure continuous security and compliance
 - Manage hundreds of thousands of endpoints, physical and virtual, regardless of location, connection type or status
 - Automatically manage patches for multiple operating systems and applications
-

In a world where the number of endpoints and the threats that can compromise them is growing at an unprecedented rate, IBM Tivoli® Endpoint Manager for Security and Compliance provides unified, real-time visibility and enforcement to protect your complex and highly distributed environment.

Designed to ensure endpoint security across the organization, Tivoli Endpoint Manager for Security and Compliance can help your organization both protect endpoints and assure regulators that you are meeting security compliance standards. It delivers an easy-to-manage, quick-to-deploy solution that supports security in an environment that is likely to include a large variety and large numbers of endpoints—from servers to desktop PCs, “roaming” Internet-connected laptops, and specialized equipment such as point-of-sale (POS) devices, ATMs and self-service kiosks.

Tivoli Endpoint Manager for Security and Compliance can reduce the costs and complexity of IT management as it increases business agility, speed to remediation, and accuracy. Its low impact on endpoint operations can enhance productivity and improve the user experience. By constantly enforcing policy compliance wherever endpoints roam, Tivoli Endpoint Manager for Security and Compliance helps reduce risk and increase audit visibility for continuous compliance.



Addressing security needs across the organization

Tivoli Endpoint Manager for Security and Compliance addresses security challenges associated with desktop and distributed environments. By providing endpoint management and security in a single solution, it helps ensure continuous protection and compliance. For example, it can dramatically shrink gaps in security exposures by applying software patches in minutes. And it can help bridge the gap between functions such as those establishing and executing strategy and policy, those managing devices in real-time, and those generating reports on security and compliance issues.

Among the capabilities of Tivoli Endpoint Manager for Security and Compliance are its ability to:

- Provide accurate, precise and up-to-the minute visibility into, and continuous enforcement of security configurations and patches.
- Centralize management of third-party anti-malware and firewall protection.
- Provide out-of-box best practices that meet U.S. Federal Desktop Configuration Control (FDCC) regulations and Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs).
- Support Security Content Automation Protocol (SCAP); Tivoli Endpoint Manager is the first product certified by the National Institute of Standards and Technology (NIST) for both assessment and remediation.
- Securely transmit endpoint instructions as demonstrated through NIAP CCEVS EAL3 and FIPS 104-2, Level 2 certifications.
- Support the Open Vulnerability and Assessment Language (OVAL) standard to promote open and publicly available security content.
- Receive and act on vulnerability and security risk alerts published by the SANS Institute.
- Show trending and analysis of security configuration changes through advanced reporting.

Additional capabilities provided for all products in the Tivoli Endpoint Manager family, built on BigFix® technology, include the ability to:

- Discover endpoints that organizations may not be aware were in their environment—up to 30 percent more in some cases.
- Provide a single console for management, configuration, discovery and security functions, simplifying operations.
- Target specific actions to an exact type of endpoint configuration or user type, and using virtually any hardware or software property to do so.
- Employ a unified management infrastructure to coordinate among IT, security, desktop and server operations.
- Reach endpoints regardless of location, connection type or status with comprehensive management for all major operating systems, third-party applications and policy-based patches.

Tivoli Endpoint Manager for Security and Compliance enables automated, highly targeted processes that provide control, visibility and speed to effect change and report on compliance. Remediation cycles are short and fast—with malware and virus issues addressed with rapid patch management capabilities.

Delivering a broad range of powerful security functions

Tivoli Endpoint Manager for Security and Compliance includes the following key functions—and gives you the ability to easily add other targeted functions as needed, without adding infrastructure or implementation costs.

Patch management

Patch management includes comprehensive capabilities for delivering patches for Microsoft® Windows®, UNIX®, Linux® and Mac OS and for application vendors such as Adobe®, Mozilla, Apple and Java™ to distributed

endpoints—regardless of their location, connection type or status. A single management server can support up to 250,000 endpoints, shortening times for patches with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks. Real-time reporting provides information on which patches were deployed, when they were deployed, and who deployed them, as well as automatic confirmation that patches were applied for a complete closed-loop solution to the patching process.

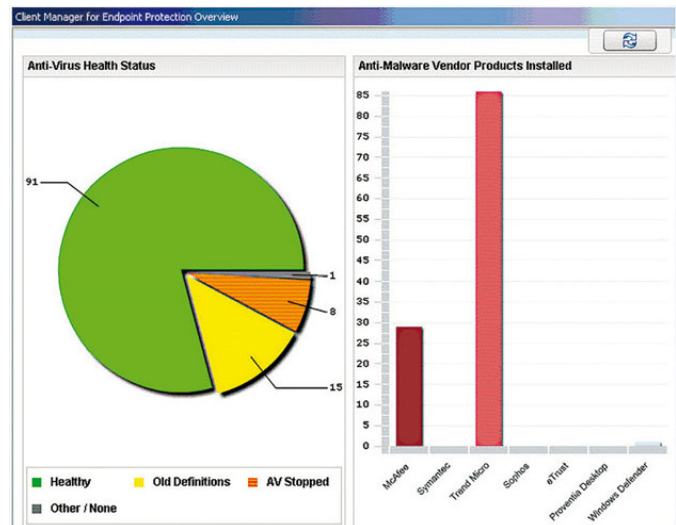
Security configuration management

Validated through the National Institute of Standards and Technology, the solution's security configuration features provide a comprehensive library of technical controls that can help you achieve security compliance by detecting and enforcing security configurations. Policy libraries support continuous enforcement of configuration baselines; report, remediate and confirm remediation of non-compliant endpoints in real time; and ensure a verified real-time view of all endpoints.

This feature delivers meaningful information on the health and security of endpoints regardless of location, operating system, connection (including wired computers or intermittently connected mobile laptops), or applications installed. It helps consolidate and unify the compliance life cycle, reducing endpoint configuration and remediation times.

Vulnerability management

Vulnerability management enables you to discover, assess and remediate vulnerabilities before endpoints are affected. The feature assesses systems against standardized open source security language (OVAL) vulnerability definitions and reports on non-compliant policies in real-time. The result is enhanced visibility and full integration at every step in the entire discover-assess-remediate-report workflow.



Tivoli Endpoint Manager for Security and Compliance provides reports that help organizations visualize the issues that impact the effectiveness of security and compliance efforts.

IT staff can identify and eliminate—using automated or manual actions—known vulnerabilities across endpoints. By using a single tool to both discover and remediate vulnerabilities, administrators can increase speed and accuracy, shortening remediation cycles for patch deployment, software updates and vulnerability fixes. Administrators can extend security management to mobile clients on or off the network—setting alarms to quickly identify rogue assets and taking steps to locate them for remediation or removal.

Asset discovery

With Tivoli Endpoint Manager for Security and Compliance, asset discovery is no longer a “bean counting” snapshot exercise. It creates dynamic situational awareness about changing conditions in the infrastructure. The ability to scan the entire network frequently delivers pervasive visibility and control to help ensure that organizations quickly identify all IP-addressable devices—including virtual machines, network devices and peripherals such as printers, scanners, routers, and switches in addition to computer endpoints—with minimal network impact. This function helps maintain visibility into all enterprise endpoints, including mobile laptop and notebook computers that are roaming beyond the enterprise network.

Multivendor endpoint protection management

This feature gives administrators a single point of control for managing third-party endpoint security clients from vendors such as Computer Associates, McAfee, Sophos, Symantec and Trend Micro. With this centralized management capability, organizations can enhance the scalability, speed and reliability of protection solutions. The feature monitors system health to ensure that endpoint security clients are always running and that virus signatures are updated. In addition to providing a unified view of disparate technologies, it facilitates migrating endpoints from one solution to another with “one-click” software removal and reinstall. Closed-loop verification ensures that updates and other changes are completed, including Internet-enabled verification for endpoints disconnected from the network.

Network self-quarantine

Tivoli Endpoint Manager for Security and Compliance automatically assesses endpoints against required compliance configurations—and if the endpoint is found to be out of compliance, the solution can configure the endpoint so that it

is placed in network quarantine until compliance is achieved. The Tivoli Endpoint Manager server has management access to the endpoint, but all other access is disabled.

Anti-malware and web reputation service (optional add-on)

Deep integration with Trend Micro’s Core Protection Module (CPM) provides features to guard endpoints against viruses, Trojan horses, worms, spyware, rootkits, new malware variants and malicious websites by querying real-time, in-the-cloud threat intelligence to nearly eliminate the need for signature files on the endpoint. Web reputation technology prevents users from accessing malicious websites, whether by their own actions or by hidden, automated actions performed by malware.

The Tivoli Endpoint Manager family

You can further consolidate tools, reduce the number of endpoint agents, and lower your management costs by extending your investment in Tivoli Endpoint Manager for Security and Compliance to include other components in the Tivoli Endpoint Management family. Because all functions operate from the same console, management server and endpoint agent, adding more services is a simple matter of a license key change.

- **Tivoli Endpoint Manager for Power Management**— This option enables enforcement of energy conservation policies across the organization, with the granularity necessary to enable application of policies to a single computer.
- **Tivoli Endpoint Manager for Lifecycle Management**— This comprehensive and powerful approach addresses today’s convergence of IT functions by providing real-time visibility into the state of system endpoints and giving administrators advanced functionality for managing those endpoints.

Tivoli Endpoint Manager: Built on BigFix technology

The power behind all Tivoli Endpoint Manager functions is a unique, single-infrastructure approach that distributes decision making out to the endpoints, providing extraordinary benefits across the entire solution family, with features that include:

- **An intelligent agent**—Tivoli Endpoint Manager utilizes an industry-leading approach that places an intelligent agent on each endpoint. This single agent performs multiple functions including continuous self-assessment and policy enforcement—yet it has minimal impact on system performance. In contrast to traditional client-server architectures that wait for instructions from a central control point, this agent initiates actions in an intelligent manner, sending messages upstream to the central management server and pulling patches, configurations or other information to the endpoint when necessary to comply with a relevant policy. As a result of the agent's intelligence and speed, the central management server always knows the compliance and change status of endpoints, enabling rapid and up-to-date compliance reporting.
- **Reporting**—The single, unified console built into Tivoli Endpoint Manager orchestrates a high level of visibility that includes real-time and continuous reporting and analysis from the intelligent agents on the organization's endpoints.
- **Relay capabilities**—Tivoli Endpoint Manager's scalable and lightweight architecture allows any agent to be configured as a relay between other agents and the console. This relay function allows the use of existing servers or workstations to transfer packages across the network, reducing the need for servers.
- **IBM Fixlet® messages**—The Fixlet Relevance Language is a published command language that enables customers, business partners and developers to create custom policies and services for endpoints managed by Tivoli Endpoint Manager solutions.

Extending the Tivoli commitment to security

Tivoli Endpoint Manager for Security and Compliance is part of the comprehensive IBM security portfolio, helping address security challenges across the organization. Supporting the instrumented, interconnected and intelligent IT operations of a smarter planet, IBM security solutions help ensure real-time visibility, centralized control and enhanced security for the entire IT infrastructure, including its globally distributed endpoints.

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 Security and Compliance, 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.



© Copyright IBM Corporation 2011

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

Produced in the United States of America
February 2011
All Rights Reserved

IBM, the IBM logo, ibm.com, BigFix and Tivoli are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

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.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

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