Keeping distributed endpoints safe and compliant

IBM Tivoli Endpoint Manager built on BigFix technology provides global control and visibility

Highlights

- Address management and compliance challenges while enhancing endpoint security
- Provide up-to-date visibility and control from a single management console
- Automatically manage patches for multiple operating systems and applications
- Enhance ROI for the distributed IT infrastructure

In today's far-reaching environments, where the numbers and varieties of servers, desktops, laptops, and specialized equipment such as point-of-sale (POS) devices, ATMs and self-service kiosks—known collectively as "endpoints"—are growing at unprecedented rates, traditional protection schemes such as firewalls are no longer enough. With rapidly increasing numbers of remote workers and roaming devices, there is no well-defined perimeter. The perimeter, by necessity, must be the endpoint itself.

Endpoints, by their very nature, are highly vulnerable to attack—including system damage inflicted by malware, theft by phishing, privacy infringements through social networking, or loss of productivity due to spam, interruptions, and system instabilities. These vulnerabilities can represent significant risk—including loss of control over the endpoint and the risk of losing valuable data. And they likely are present to one degree or another on every endpoint in your organization.

Many exposures are simply the result of endpoints that lack critical patches or have configuration errors that leave them open to attack. The Stuxnet virus outbreak, for example, exploited well-known vulnerabilities tied to the use of USB drives and the Microsoft® Windows® "autoplay" feature as an attack vector, both of which could have been eliminated through the consistent application of configuration and update policies organization-wide.

The pains caused by security issues, however, are not only in the attacks, but also in the way that organizations protect themselves. Protection can be costly, complex and time consuming, stretching IT staff thin and driving costs even higher. After security is in place, many organizations have to prove compliance with internal policies, security standards and government regulations. In addition to the pain involved in achieving initial compliance, "compliance drift" is another key concern. Once compliance levels are attained, organizations must ensure that they are continuously maintained.

IBM Tivoli® Endpoint Manager, built on BigFix® technology, can meet all of these needs, scaling from small to large organizations using the same easily deployed technology. It provides real-time visibility and control over each endpoint's status, remediating issues to help ensure continuous security and compliance.

Visibility and control are the foundation of security

Organizations can have as few as a hundred or as many as several hundred thousand endpoints that must be kept secure in order to effectively manage risk, contain costs and maintain compliance. The challenges in managing such a large, diverse collection of technology lie in knowing how many and what types of endpoints you have, verifying and updating patch and security policies across all endpoints, and confirming compliance with internal IT and external regulatory policies—and doing it all fast enough to make a real difference in your security posture.

In a large and complex environment where threats come from multiple directions and individual endpoints are frequently targeted, where do you turn? How do you manage thousands of moving targets that are so diverse that they are seemingly unmanageable?

The answer is to deploy a single, unified tool that not only addresses the risks associated with security threats but also controls cost, complexity and staff burden while meeting compliance mandates. Organizations need a simplified, streamlined, highly scalable visibility and enforcement tool that delivers continuous protection designed for today's distributed environments.

The ideal endpoint management tool provides smarter, faster, automated management capabilities that leverage the opportunities available in today's interconnected world while adapting to the inherent challenges presented by this environment. With the right tool, you can see and protect all of your organization's physical and virtual endpoints, whether desktop PCs, "roaming" Internet-connected laptops, servers or specialized equipment such as point-of-sale devices, ATMs and self-service kiosks. You can help ensure security for your environment whether it is based on Microsoft Windows, UNIX®, Linux® or Mac operating systems—or any combination—from the same console, utilizing the same management infrastructure.

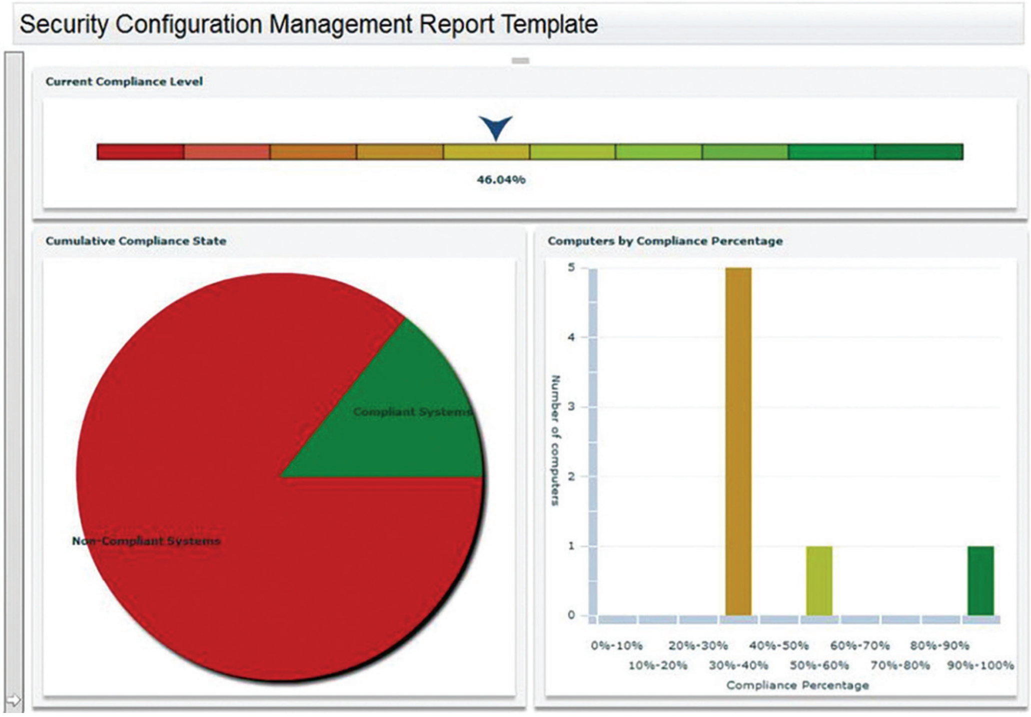
Tivoli Endpoint Manager delivers rapid results

Tivoli Endpoint Manager deploys in hours or days, depending on the complexity of your infrastructure, to deliver comprehensive endpoint security capabilities across the organization. This unified solution delivers endpoint management for hundreds of thousands of endpoints via a single console and single management server, rapidly exposing security risks by identifying and remediating vulnerabilities in real time.

The solution's discovery capabilities identify endpoints on the network that you may not know you have, including rogue endpoints that do not belong on your network and other endpoints that are not currently under management. Tivoli Endpoint Manager's intelligent agent deploys quickly and identifies current patch and configuration levels, comparing them against defined policies. It then quickly and accurately applies operating system and application updates regardless of the endpoint's location, connection type or status, and continuously enforces policy compliance, even if endpoints are not connected to the network. Vulnerability management capabilities quickly identify and eliminate vulnerabilities, assessing and remediating managed endpoints against known vulnerabilities using predefined policies.

Tivoli Endpoint Manager's unique intelligent agent continuously enforces security policies regardless of endpoint connectivity. Traditional endpoint management solutions utilize agents that depend entirely on instructions received from a central command-and-control server. The intelligent agent built into the IBM solution autonomously initiates update and configuration actions to keep the endpoint current and compliant with organizational policies, which are encapsulated in IBM Fixlet® messages. Agents download relevant patch, configuration or other content to the endpoint only when needed, while also continuously monitoring policy compliance and sending status updates to the management console as changes are detected.

The Tivoli Endpoint Manager agent constantly monitors endpoint compliance, communicating endpoint status and providing real-time visibility through a single, centralized console. And by leveraging a continually updated policy database of thousands of IBM Fixlet messages, as well as providing the ability for customers to create their own Fixlets, Tivoli Endpoint Manager's management server always contains current endpoint compliance, configuration and change status, enabling real-time reporting.



Reporting via a centralized console provides real-time visibility into configuration and compliance status in a variety of easy-to-understand formats.

Tivoli Endpoint Manager addresses a full range of security needs

Tivoli Endpoint Manager provides key security capabilities including:

- **Security standards support:** Provides out-of-box best practices that meet U.S. Federal Desktop Configuration Control (FDCC) regulations. It also supports the full range of Security Content Automation Protocol (SCAP) standards and the Open Vulnerability and Assessment Language (OVAL) standard to promote open and publicly available security content. The solution supports the Secure Content Automation Protocol (SCAP) and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), and it can receive and act on vulnerability and security risk alerts published by the SANS Institute.
- **Patch management:** Provides comprehensive capabilities for delivering patches from a full range of operating system and application vendors to distributed endpoints, shortening times for patches and updates with no loss of endpoint functionality, even when connected over low-bandwidth, globally distributed networks or if endpoints roam outside of the organization's firewall.
- **Security configuration management:** Delivers meaningful information on the health and security of endpoints regardless of location, operating system, applications installed or connection type.
- **Vulnerability management:** Assesses endpoints against standardized, OVAL-based security vulnerability definitions and reports on non-compliance in real time to support the elimination of known vulnerabilities across endpoints.
- **Client manager for endpoint protection:** Provides a single point of control for managing third-party anti-virus and firewall products from vendors including Computer Associates, McAfee, Symantec and Trend Micro, enabling organizations to enhance the scalability, speed and thoroughness of protection solutions.
- **Network self-quarantine:** Automatically assesses the endpoint against required compliance configurations—and if the endpoint is found to be out of compliance, the solution can configure the endpoint to be put in network quarantine until compliance is obtained. The Tivoli Endpoint Manager server is provided with management access, but all other access is disabled.
- **Endpoint firewall:** Enables administrators to enforce policies based on endpoint location, control network traffic based on source and destination IP addresses, regulate inbound and outbound endpoint communications, and quarantine endpoints when necessary.
- **Asset discovery:** Creates dynamic visibility into changing conditions in the infrastructure, with the ability to deliver pervasive visibility and control, including quick identification of unmanaged network devices for further investigation or to support automatic agent installations to rapidly bring "rogue" endpoints under management.

A unified solution is the key to endpoint management success

The visibility and control provided by Tivoli Endpoint Manager can be key to an organization's overall success. Organizations today need sophisticated, automated tools for harvesting increasingly time-sensitive data about their endpoints and to define, deploy and enforce security policies that protect their endpoints and continuously enforce compliance.

The saying that "you can't manage what you can't see" is as true in the realm of security as it is anywhere else. To properly remediate vulnerabilities, you must first know which endpoints are at risk. Many failed audits result from poor visibility into endpoint vulnerabilities due to endpoint configuration "drift," or the inability to rapidly deploy (and confirm) the application of patches and updates.

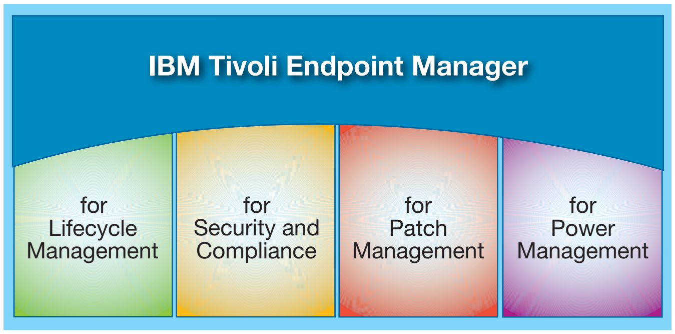
A solution with a single console can help organizations move to a unified management approach, enhancing visibility and control. It can help bridge the gap between the establishment of security strategy and policy, execution of that strategy, real-time operational management of endpoints, and security and compliance reporting, for example.

Tivoli Endpoint Manager can dramatically shrink gaps in security exposures by quickly and accurately effecting changes across the infrastructure. It eliminates the clutter of multiple management tools that make comprehensive visibility and control difficult or impossible, providing a single management infrastructure that coordinates efficiently among IT, security, desktop and server operations, effecting change, fixing problems, answering questions and reporting on compliance throughout the organization.

Tivoli Endpoint Manager helps reduce security risks, management costs and management complexity as it increases the speed and accuracy of remediation while improving the productivity and satisfaction of end users. The single agent, single console and single management server approach streamlines processes and increases reliability. The solution delivers rapid time-to-value through functions such as patch management and asset discovery as well as long-term ROI by increasing operational efficiencies, enabling management infrastructure consolidation and improving IT productivity.

IBM Tivoli Endpoint Manager is a family of products that all operate from the same console, management server and endpoint agent. This approach helps you consolidate tools, reduce the number of endpoint agents, and lower your management costs. And adding more services is a simple matter of a license key change. The IBM Tivoli Endpoint Manager family includes:

- IBM Tivoli Endpoint Manager for Lifecycle Management
- IBM Tivoli Endpoint Manager for Security and Compliance
- IBM Tivoli Endpoint Manager for Patch Management
- IBM Tivoli Endpoint Manager for Power Management



IBM Tivoli Endpoint Manager is a family of products that all operate using the same console, management server and endpoint agent.

IBM security solutions support today's organizations

Tivoli Endpoint Manager is part of the comprehensive IBM security portfolio, helping organizations address security challenges for users and identities, data and information, applications and processes, networks, servers and endpoints, and physical infrastructures. By enhancing real-time visibility and control, enabling power management and improving endpoint security and management, it supports today's ever-expanding, smarter data centers. Facilitating 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.

For more information

To learn more about IBM Tivoli Endpoint Manager, 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 lifecycle management, and is backed by world-class IBM services, support and research.

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.

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

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

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.

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.

Please Recycle

Tivoli. software