IBM Software

Select the right solution for endpoint management

Enhance visibility and control for hundreds of thousands of distributed endpoints

Managing thousands of computing endpoints, including workstations, servers and roaming mobile devices such as laptops, smartphones and tablets, presents IT organizations with a formidable challenge. With conventional management methods, even simple questions such as, "How many mobile laptops do we have?", "What OS versions are our desktop systems running?" or "Are our patches up-to-date?" can take days to obtain and generate inaccurate, incomplete responses.

That's why, as organizations attempt to consolidate and eliminate redundant and non-performing management tools, enhance security and compliance, and reduce costs and IT workload, many are looking for ways to meet today's complex endpoint management needs with IT operations and security automation.

Organizations are seeking ways to overcome poor visibility into their endpoint infrastructure so they can understand needs, gaps and opportunities for improvement. They are looking for ways to speed and simplify the deployment of new software, software updates and critical security patches, maintain and prove compliance with evolving industry and government regulations, and protect an ever-expanding and often porous perimeter that is vulnerable to attack and security risk.

In a world accustomed to multiple, fragmented technologies and point solutions, organizations need a unified approach that supports endpoint management across heterogeneous devices and operating systems. They need fast deployment and rapid time to value. They need an open architecture that allows customization and the creation of company-specific policies without extensive programming and scripting. And when the environment faces threats, they need agile, real-time endpoint visibility, protection, rapid remediation and reporting capabilities.

An effective endpoint management solution can meet all these goals as it simplifies management processes, enhances endpoint control and centralizes views with a single, easy-to-use graphical user interface. It can deliver these management capabilities for any number of physical and virtual endpoints ranging from servers to desktops, laptops, smartphones and tablets, plus specialized equipment such as point-of-sale devices, ATMs and self-service kiosks.

Endpoint management can play a key role in effectively delivering secure, stable IT services 24×7 to customers, employees, business partners, regulators, investors and other constituents. The highly exposed nature of today's IT infrastructures is changing how organizations manage endpoints, processes and data. An endpoint management solution can be fundamental to the transformation of IT functions from back-end operations to key services that are closely integrated with business success, compliance with internal security policies, and effective process execution.

Getting started with endpoint management

This buyer's guide outlines features and capabilities that comprise an effective endpoint management solution:

- Endpoint discovery, inventory and usage analysis
- Patch management and endpoint software distribution
- Security and compliance
- Mobile device management
- Green IT
- Management system architecture

This guide discusses the benefits of each capability and provides checklists to help you evaluate whether or not a particular vendor's solution addresses each of these areas effectively. You will also find a list of attributes and capabilities you should look for in selecting a provider that can support the full breadth of your endpoint management requirements.

Endpoint discovery, inventory and usage analysis

Gathering information about endpoints should be more than a number-counting, "snapshot" exercise conducted periodically. It should create dynamic, near real-time awareness about changing conditions in the infrastructure—with pervasive visibility and control to quickly identify all IP-addressable devices in the organization and the applications installed on them.

The optimal solution can drill-down to uncover details across vast infrastructures with hundreds of thousands of endpoints, rapidly delivering aggregated statistics and usage information. It helps maintain visibility into all endpoints, including mobile devices that roam outside the organization's network. It brings newly discovered endpoints under management and has minimal impact on network operations. And it should do all of this as close to real-time as possible.

Endpoint discovery, inventory and usage analysis

Look for a solution that:	**IBM**	**Other**
Includes both agent-based and agentless distributed scanning architecture for low-impact, low-latency device detection as well as deep inspection and reporting	✓	
Quickly identifies all IP-addressable devices including network devices and peripherals such as printers, scanners, routers and switches in addition to computer endpoints	✓	
Discovers undocumented endpoints within the environment and identifies suspicious "rogue" devices	✓	
Provides near real-time reporting of open ports and services in use	✓	
Provides discovery and inventory management capabilities from a single console	✓	
Supports ad hoc queries to endpoints—for example: "Get me the serial numbers of all computer monitors"—and delivers results in minutes with minimal impact at scale	✓	
Reaches endpoints regardless of their location, on- or off-network, and keeps inventory data current, even for endpoints not constantly connected to the network	✓	
Provides accurate, in-depth and detailed inventory data that includes all hardware, configuration, and software properties	✓	
Supports searching, browsing, and editing of a software identification catalog containing more than 100,000 signatures out-of-the-box, and is kept current based on changes in the software industry	✓	
Allows easy, wizard-based customization of the software identification catalog to include tracking of home-grown and proprietary applications	✓	
Provides drill-down information about the software publishers, titles and applications found on endpoints	✓	
Includes software metering that aggregates historical statistics and usage information	✓	
Correlates information on software use with license information for immediate, accurate and automated license "true-ups" that identify non-compliant instances, then flags them for removal	✓	
Provides rich asset data for reporting and integrating with other enterprise systems that need accurate, up-to-date inventory (for example, service desk, asset management system, inventory warehouse, configuration management databases)	✓	
Enables ease of implementation and use, providing entry-level software asset management features while enabling adoption of more sophisticated solutions	✓	
Provides tight integration with endpoint security and compliance management	✓	
Supports both physical and virtual software use analysis, including Microsoft App-V virtual applications	✓	

Patch management and endpoint software distribution

Increasing infrastructure complexity, proliferation of management tools, and overloaded IT personnel can overwhelm efforts to manage a rapidly growing base of endpoint devices and platforms. Organizations need a comprehensive, unified management solution that reduces the clutter, inefficiency and expense of multiple tool sets as it delivers real-time visibility and control. Such a solution can optimize processes by bringing them together under a single management umbrella—while helping reduce cost and risk and enhancing management effectiveness.

An effective solution provides policy-based installation of security updates and software packages, closed-loop verification and the ability to manage software distribution across multiple platforms from a single point of control. The same management console deploys critical operating system and software patches, enabling system administrators to easily maintain the desired state of managed endpoints. And it shrinks OS deployment and user profile migration time, reduces risks associated with non-compliant configurations, and minimizes impact on end users—while simplifying deployment of new workstations, laptops, servers and mobile devices.

Patch management

Look for a solution that:	**IBM**	**Other**
Provides automatic patch management from a single management console	✓	
Automatically manages patches for multiple operating systems, including Microsoft Windows, UNIX, Linux and Mac OS, plus smartphones and tablets from the same console and server	✓	
Automatically manages patches for applications from a wide range of vendors, including Microsoft, Apple, Adobe, Mozilla and Java	✓	
Reduces remediation cycles from weeks to days or hours, minimizing security and compliance risk	✓	
Enables patch management for endpoints on or off the network, including roaming, Internet-connected devices	✓	
Provides consistent functionality even over low-bandwidth or globally distributed networks	✓	
Increases first-pass patch success rates to as much as 95 to 99 percent (from a typical 60 to 75 percent)—and confirms successful remediation	✓	
Removes patch management overhead by providing pre-tested and packaged patch policies and making them automatically available to patch administrators	✓	
Allows grouping of patches into a single deployment task to simplify management, automatically resolving dependencies if necessary	✓	
Downloads and applies only the patches relevant to each endpoint	✓	
Allows system administrators to rapidly create and deploy custom patches	✓	
Enhances visibility into patch compliance with flexible, real-time graphical monitoring and reporting	✓	

Patch management

Look for a solution that:	IBM	Other
Delivers information on patch status (for example: Needs patch, patch is pending or running, patch was installed successfully, patch installation failed)	✓	
Delivers information on which patches were deployed, when they were deployed and who deployed them	✓	
Automatically compares endpoint compliance against defined policies, such as mandatory patch levels	✓	
Detects and remediates issues where a previously installed patch has been rolled back or overwritten. Allows automatic reapplication of uninstalled patches	✓	
Allows making patches available as "offers" to users with or without mandatory implementation dates to minimize disruptions	✓	
Allows patches to be grouped and rapidly installed during defined change windows	✓	
Allows optional patch dialog window suppression and delayed/scheduled reboots	✓	

Organizations are more widely distributed today than ever, making IT management tasks like distributing and managing endpoint software extremely challenging. These organizations need robust capabilities for quickly and reliably delivering, and managing business-critical applications on a full spectrum of endpoints.

Endpoint software distribution

Look for a solution that:	IBM	Other
Provides management of software distribution across multiple platforms from a single, unified point of control	✓	
Supports policy- and computer group-based installation of new and updated software packages across distributed environments	✓	
Delivers closed-loop verification of software installation/de-installation	✓	
Supports user self-provisioning and de-provisioning of authorized applications and software packages	✓	
Supports local pre-caching of software packages to improve installation reliability	✓	
Eliminates the need to duplicate files for software distribution	✓	
Supports "follow the user" software distribution policies	✓	
Provides simple yet powerful customization capabilities for accurate targeting and deployment of software packages	✓	

Endpoint software distribution

Look for a solution that:	**IBM**	**Other**
Minimizes network impact via policy-driven bandwidth throttling, both static and dynamic, across all OS platforms, including the ability to throttle against actual available network link bandwidth	✓	
Maintains configuration files such as Microsoft Software Transform (MST) and Microsoft Software Patch (MSP) files separately from core software components to efficiently handle multiple package configurations	✓	
Is compatible with incumbent software distribution tools and package formats	✓	
Supports "bare metal" operating system deployment for new workstations, laptops and servers throughout the network as well as OS migration and refresh for existing endpoints	✓	
Utilizes the endpoint management core infrastructure for OS migration, eliminating the costs associated with maintaining a standalone OS deployment infrastructure	✓	
Shrinks deployment and migration time with fully automated operations including remote wake-up support and deployment scheduling	✓	
Deploys hardware-independent images to machines from multiple hardware vendors, injecting appropriate device drivers as needed	✓	
Enables in-place migration of user profiles and data	✓	
Integrates OS deployment with security baselines and configuration provisioning requirements, including "top off" patching so that systems are ready to use immediately	✓	
Provides multiplatform remote control and troubleshooting	✓	
Puts real-time endpoint data at administrators' fingertips with remote diagnostics capabilities that can simplify and streamline help-desk calls and problem resolution	✓	
Targets specific actions to an exact type of endpoint configuration or user type	✓	
Provides remote discovery and analysis of applications installed on endpoints	✓	
Allows administrators to establish role-based access to support different user responsibilities and line of business requirements	✓	
Simplifies and operationalizes security by embedding security practices and compliance initiatives as part of the IT operations process	✓	

Security and compliance

In today's far-reaching environments, an organization often has no well-defined perimeter, leaving endpoints highly vulnerable to attack. What's more, the speed of attacks is increasing, as is the speed at which new vulnerabilities are being introduced—far beyond what most tools can handle today. Can you detect and correct vulnerabilities fast enough to protect your servers, PCs and other endpoints from being compromised?

While most organizations are focused on protecting their users from the threat of incoming malware and viruses, a growing number of organizations also have to protect mobile users, securing sensitive data from the inside. Not all data breaches begin with malicious intent: Users routinely copy sensitive information to devices, such as USB drives, memory cards, cloud-based synchronization services and mobile devices. Many employees now work from laptops that routinely leave the office with sensitive data on them.

Faced with these challenges, organizations need a data loss prevention (DLP) solution that can be easily deployed as part of their existing endpoint security infrastructure. They need a unified solution that not only addresses the risks associated with security threats but also controls cost, complexity and staff burden while meeting compliance mandates. Such a solution can help the organization both protect endpoints and assure that compliance with internal security policies is being met.

Endpoint security

Look for a solution that:	**IBM**	**Other**
Manages the configuration of physical and virtual endpoints regardless of location, operating system, applications installed or connection (including wired computers or intermittently connected mobile devices)	✓	
Remediates endpoints to a compliance baseline and then continuously enforces configuration policies on or off the network	✓	
Provides accurate, up-to-the minute visibility into and continuous enforcement of security configurations and patches from a single management console	✓	
Enables real-time response to zero-day attacks through ad hoc, closed-loop remediation, allowing administrators to quickly and easily create custom remediation policies and implement them across the organization within hours, for endpoints both on and off the network	✓	
Contains a comprehensive library of technical controls based on well-known best practices that help achieve security compliance by detecting and enforcing security configurations	✓	
Supports the Security Content Automation Protocol (SCAP)	✓	
Uses predefined, out-of-the-box policy definitions based on the Open Vulnerability and Assessment Language (OVAL) standard to assess managed endpoints against known vulnerabilities	✓	
Capable of acting on vulnerabilities and security risk alerts published by the SANS Institute	✓	
Maps vulnerabilities to industry standards to provide Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS) references and links to the National Vulnerability Database (NVD)	✓	

Endpoint security

Look for a solution that:	**IBM**	**Other**
Provides out-of-the-box checklists containing over 5,000 standard configuration settings mapped to industry standards for Windows, UNIX and Linux	✓	
Automates and simplifies technical controls compliance reporting for Sarbanes-Oxley, HIPAA, UK Financial Services Act and other regulations	✓	
Provides out-of-the-box best practices that meet U.S. Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baseline (USGCB) regulations	✓	
Provides out-of-the-box best practices that meet Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)	✓	
Identifies and eliminates known vulnerabilities using automated policy enforcement or manual deployment	✓	
Enables easy integration with related technologies such as help-desk systems, asset management systems, configuration management databases (CMDBs) and security information and event management (SIEM) systems	✓	
Sets alarms to quickly identify rogue or misconfigured endpoints and takes steps to locate them for remediation or removal	✓	
Can automatically place out-of-compliance endpoints in network quarantine while keeping them under management until remediation is complete	✓	
Provides wizards for custom policy formulation, reporting and enforcement	✓	
Is certified by the National Institute of Standards and Technology (NIST) for both assessment and remediation	✓	
Enables quick customization with minimal lines of code through an easy to use API that supports multiple platforms using the same language	✓	
Provides a central hub for all systems management automation tools, allowing administrators to use the tools that they know (that is, shell scripting in UNIX, batch files in Windows, Apple script, and so on)	✓	
Supports administrator skill levels from beginner (with a wizard to create scripts without having to know the tool's language) to expert (with extreme flexibility in customization)	✓	
Provides tight integration with endpoint life cycle operations management	✓	

It is common for an organization to need compliance information on a particular platform or type of endpoint, on a particular organizational or geographical segment or on a specific regulatory or governance objective across all endpoints. Meeting this need requires comprehensive reporting capabilities that leverage warehousing analytics and asset data to ensure rapid, timely and easy-to-use reports and views.

Reporting and analytics

Look for a solution that:	**IBM**	**Other**
Collects and archives automated security check results to help identify configuration issues and report levels of IT security-related compliance	✓	
Provides analytics capabilities that support enforcement of the organization's technical and configuration policies by monitoring, reporting and tracking progress, and determining the success of security initiatives	✓	
Provides historical reports to determine progress being made toward compliance goals	✓	
Delivers meaningful, real-time and historical reports on the health and security of endpoints for use in the remediation of non-compliant endpoints and confirmation of remediation	✓	
Provides overview dashboards and executive rollups showing historical security compliance and hot spots, with the ability to drill down for detailed information	✓	
Provides actionable reports consolidated by remediation technique (such as a specific patch), not just a "laundry list" of overlapping, often redundant vulnerabilities	✓	
Identifies, manages and reports on policy exceptions and deviations	✓	
Provides a full range of reports for managing IT policy checks, including compliance status and history, reports by computer and computer group, and exception reports	✓	
Enables the creation of flexible, on-demand, ad hoc custom queries and reports	✓	
Provides report flexibility, including report filters (for example, historical compliance, computer metadata, checklist metadata, and so on), report column management, actual measured versus desired values, report exports, saved reports and more	✓	
Enables users to easily create custom checklists within minutes by combining included best practice checks with custom checks	✓	
Shows trending and analysis of historical configuration compliance and security changes through advanced reporting	✓	
Bases analysis on infrastructure views that can be defined in multiple ways, from an individual device to groups of devices to the entire infrastructure	✓	

Reporting and analytics

Look for a solution that:	**IBM**	**Other**
Includes a separate security analytics data warehouse to store historical compliance data	✓	
Provides a holistic view of compliance status plus vulnerability status in the same report or online view	✓	
Supports audit requests by providing a historical state versus current state view	✓	
Supports a reporting server for auditors, with read-only access and access to selected information	✓	
Restricts access to endpoints and reports through user permissions and roles	✓	
Uses the same console, architecture and agent as IT operations uses to manage endpoints	✓	

Recent data breaches highlight the urgency of protecting sensitive data from accidental or intentional misuse and loss. Faced with these challenges, organizations need a robust endpoint protection and data loss prevention (DLP) solution that integrates easily into the existing endpoint management infrastructure, effectively addressing the obstacles to deploying effective data protection. Deploying a unified endpoint security infrastructure can help reduce complexity and save administrative time and costs.

Endpoint protection

Look for a solution that:	**IBM**	**Other**
Provides a consolidated, unified approach to delivering and managing antivirus, anti-spyware, firewall and encryption services for leading products from multiple vendors, such as Symantec, McAfee, Trend Micro, Microsoft and Sophos	✓	
Monitors system health to ensure that endpoint protection clients are always running and that virus signatures are updated	✓	
Facilitates migrating endpoints from one security solution to another with one-click software removal and reinstall	✓	
Uses closed-loop verification to ensure that security settings have been applied and enforced and that updates and other changes are completed; provides Internet-enabled verification for endpoints disconnected from the network	✓	
Prevents users from accessing malicious websites, whether by their own actions or by hidden, automated actions performed by malware on their computer	✓	

Endpoint protection

Look for a solution that:	**IBM**	**Other**
Utilizes cloud-based web reputation technology that dynamically rates millions of individual web pages every day to protect against web-based malware including Web 2.0 threats and data-stealing malware	✓	
Guards endpoints against viruses, Trojan horses, worms, spyware, rootkits, new malware variants and malicious websites	✓	
Identifies and completely removes discovered spyware, including hidden rootkits and remnants	✓	
Provides a fully integrated antivirus and firewall solution with the overall endpoint management console and infrastructure, eliminating the costs and complexity associated with maintaining a standalone antivirus and firewall deployment infrastructure	✓	
Provides integrated data loss prevention (DLP) capabilities deployed using the same single console and single agent infrastructure	✓	
Includes DLP to secure data on all devices, enforce security policies so that users can access sensitive data for their jobs but not misuse or lose that data, and help comply with data privacy regulations	✓	
Protects against the misuse of data based on keywords, regular expressions and configurable rules that can look for specific formatting or even coding (for example Java code) and respond accordingly	✓	
Includes pre-defined templates designed to identify and control data according to specific regulations, such as GLBA, HIPAA, PCI-DSS, SB-1386, PCI and US PII	✓	
Provides multichannel monitoring and enforcement to block or allow when data is copied to or sent to a variety of delivery channels including email, clipboard, FTP, HTTP, HTTPS, SMB, IM, webmail and others, as well as monitoring physical channels such as data recorders, encryption, peer-to-peer applications, removable storage, and so on	✓	
Enables configurable response actions ranging from blocking the action and warning the end user to automated notification of administrators	✓	
Monitors and controls physical ports on endpoints and can enable or disable these ports based on device type and content-aware scanning restrictions	✓	
Includes granular device control to restrict USB removable storage device access by vendor, model and serial number of the device	✓	

Mobile device management

With powerful smartphones and tablet computers now in millions of hands, business use of these devices is increasing exponentially. These mobile endpoints give workers new levels of flexibility, and in turn drive new levels of productivity. But unlike traditional endpoints, which IT organizations have managed for years, mobile device platforms present unique management needs that do not fit the traditional endpoint management paradigm. Unable to accommodate these devices using their existing management technologies and infrastructures, IT organizations often find themselves scrambling to find an efficient and secure way to manage employee use of mobile devices in the workplace.

Rather than implementing a separate management infrastructure and processes solely for mobile devices, organizations can benefit from a single solution that provides unified endpoint management—a solution that provides high levels of application and security management across all types of endpoints while effectively accounting for the unique needs of mobile devices. The ideal unified management platform should secure and manage traditional endpoints as well as smartphones and tablet computers.

Mobile device management

Look for a solution that:	**IBM**	**Other**
Leverages a single infrastructure to deliver unified management and security for all types of enterprise endpoints, including smartphones, tablets, desktops, laptops and servers	✓	
Enables comprehensive configuration and enforcement of device settings, including password and encryption policies, email, VPN, LDAP, Wi-Fi, camera, and other settings	✓	
Safeguards enterprise data by enabling complete or selective wipes when devices are lost, stolen or decommissioned	✓	
Provides the flexibility of securing and managing devices using a combination of email-based and agent-based management while preserving the native device experience	✓	
Helps maintain compliance by identifying non-compliant devices and automatically taking corrective actions such as denying email access, deprovisioning profiles or removing VPN access	✓	

Mobile device management

Look for a solution that:	IBM	Other
Delivers full application management by reporting on installed apps, identifying blacklisted apps, and enabling app distribution via an enterprise app store	✓	
Offers enterprise-grade APIs for integration of mobile device and traditional endpoint data with other enterprise systems, such as service desks and configuration management databases (CMDBs)	✓	
Enables management over the corporate network, over the air (OTA) or via the Internet	✓	
Provides user self-service capabilities	✓	
Captures and stores detailed device data, including inventory data such as device model and serial number, usage data such as last connection time, and hardware information such as firmware and memory, as well as operating system version, location information, network details, and installed applications and certificates	✓	
Detects rooted or "jailbroken" devices	✓	
Enables administrators to distribute, install, revoke, remove and return status of third-party certificates	✓	

Green IT

Most endpoints have built-in power management features, and many end users are familiar with their controls. But relying on end users to manage an organization's power consumption is seldom enough to achieve measurable results. A more effective approach is centralized management. An ideal solution can reduce electricity usage while avoiding disruptions in systems management, with controls provided through a single, unified console.

Such a solution enables the IT organization to apply conservation policies infrastructure-wide while providing the necessary granularity to apply power management policies to a single computer if necessary. Combine power management with remote wake-up capabilities, and the result can satisfy the sometimes conflicting needs of management, which typically prefers that machines be powered down frequently to maximize energy savings, and the needs of IT, which requires machines to be on during non-working hours, when it is easiest to apply patches and updates.

Green IT

Look for a solution that:	**IBM**	**Other**
Enables management of power settings from the same centralized server and console for all endpoints running Windows and Mac operating systems	✓	
Provides out-of-the-box capabilities to deal with common power management issues, such as PC insomnia and PC narcolepsy	✓	
Provides the granularity necessary to apply policies to a single computer when necessary	✓	
Enables administrators to assign different power usage metrics to systems based on detected characteristics	✓	
Provides fine-grained controls for hibernation, standby and "save work before shutdown" options	✓	
Empowers end users with an opt-in approach that allows them to select their power profile from a menu of administrator-defined power configuration options	✓	
Engages end users in conservation initiatives through a client-side dashboard view into their individual power consumption and savings	✓	
Enables the creation of "what if" energy usage scenarios and provides green impact reports to encourage participation in conservation initiatives	✓	
Identifies and automatically fixes power profile misconfigurations	✓	
Schedules computer sleep and hibernation states to keep a limited number of computers functional enough to receive and distribute wake-up alarms to other computers in deeper states of sleep	✓	
Preserves user data by automatically saving documents prior to beginning a shutdown or sleep/standby procedure	✓	
Schedules Wake-on-LAN (WoL) to enable endpoint wake-up before the start of the workday or for scheduled maintenance, including support for remote user wake-up	✓	
Provides graphical reporting on aggregate power usage and savings, with the ability to export report data to Microsoft Excel for further analysis	✓	

Management system architecture

In most distributed environments, the numbers and types of endpoints are rising and networks are growing more complex. Visibility and control of endpoints are often poor and service levels are difficult to maintain. The resulting challenge is how to achieve an accurate and comprehensive "single source of truth" for the environment—and then use that truth for managing those vast numbers of endpoints. The solution lies in technologies that can consolidate and simplify key management services organization-wide.

By placing an intelligent agent on each endpoint, such a solution can perform functions including continuous self-assessment and policy enforcement. In contrast to traditional client-server architectures that wait for instructions from a central control point, an intelligent agent initiates actions in an autonomous 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.

This single-infrastructure approach distributes decision making out to the endpoints to shorten update cycles, improve success rates for provisioning, boost end-user productivity, and reduce IT and help-desk labor requirements.

Management system architecture

Look for a solution that:	**IBM**	**Other**
Consolidates IT operations and IT security functions in a single view, delivery model and software offering	✓	
Assesses and remediates issues using a single, multipurpose, intelligent agent	✓	
Provides continuous endpoint self-assessment and policy enforcement in real-time	✓	
Typically utilizes less than 10MB of endpoint memory	✓	
Requires on average less than two percent of CPU utilization, ensuring endpoint performance is not impacted	✓	
Autonomously assesses and enforces policies whether the endpoint is connected to the corporate network or not	✓	

Management system architecture

Look for a solution that:	**IBM**	**Other**
Provides local resources and policy-based, dynamic network bandwidth utilization throttle controls	✓	
Employs a published command language to enable customers, business partners and developers to create custom policies and services for managed endpoints	✓	
Delivers real-time visibility into all endpoints including desktops, laptops, servers, mobile devices, point-of-sale systems, ATMs and self-service kiosks	✓	
Provides an easy-to-use graphical user interface as well as an advanced command line interface (CLI) and application programming interface (API)	✓	
Supports up to 250,000 endpoints from a single management server	✓	
Manages mobile endpoints whether connected to the network or not	✓	
Manages heterogeneous platforms (Microsoft Windows, UNIX, Linux and Mac operating systems running on physical or virtual machines) plus smartphones and tablets	✓	
Uses the same infrastructure and resources to provide integrated remote control to simplify and streamline help-desk calls and problem resolution	✓	
Utilizes existing servers or workstations to stage content such as software installers and patches, reducing the need for management servers, ensuring speed of package delivery and minimizing network traffic	✓	
Allows any agent to be configured as a relay, or staging agent, between other agents and the centralized management console, optionally storing policies and content to reduce network load	✓	
Provides a vendor software solution that is certified using EAL 3 Common Criteria	✓	
Controls access through user permissions and roles to restrict access to endpoints, reports and the management console	✓	
Installs rapidly, with full deployments completed in hours or days, compared to weeks or months, even for the largest of organizations	✓	

Management system architecture

Look for a solution that:	IBM	Other
Brings newly discovered endpoints under management in minutes with a local deployment of the intelligent agent	✓	
Utilizes the same infrastructure across endpoint management capabilities, making it easy to solve today's challenges and seamlessly add other endpoint management capabilities as organizational requirements grow	✓	
Upgrades itself using its own infrastructure, enabling major product upgrades and updates in minutes or hours rather than weeks or months	✓	
Minimizes the effort to keep implementations current using integrated product and content updates	✓	
Integrates with a comprehensive management portfolio to help ensure real-time visibility, centralized control and enhanced functionality for the entire IT infrastructure	✓	
Provides native language support for Italian, German, French, Spanish, Japanese, simplified Chinese, Traditional Chinese, Portuguese, Korean and English	✓	

Selecting the right endpoint management provider

The provider you choose should be able to support the full breadth of your endpoint management requirements. Ideally, you will also want a provider that can support you throughout the process of implementing the solution. Before you select a provider, be sure to ask these questions:

Does your provider support your organizational goals through their technology?

Look for providers whose solutions align with your organization's objectives. Do their solutions promote efficiencies, reduce business service deployment time, reduce costs, enhance compliance and speed time to market?

Does your provider offer part of the total solution or the complete solution?
With a provider who is focused too narrowly on a solution that addresses only a particular environment or endpoint requirement, you can run into an "islands of management" problem. Solution costs, and the time it takes to manage multiple providers, can rise dramatically when multiple providers are involved. Look for a provider with a complete portfolio for endpoint management.

What type of global presence does your provider have?
If your organization has international offices, you should look for a provider with a global presence and proven international experience. Make sure the provider can support your offices abroad with their own local resources.

Is the solution supported by a mature support organization with the expertise and bandwidth that can be relied on when you need them?
Your provider should offer highly responsive and highly effective customer support. Find a provider who has a proven support organization to help you maximize the value of your software investment.

How sure are you of your provider's stability and staying power in today's economy?
A big issue in a challenging economy is provider stability and viability. You should consider a provider who has a long history in the industry, a solid, forward-looking strategy and the resources to withstand adverse economic times.

Can your provider deliver products that are strategically designed and technically superior?
When comparing various solutions, look for technical superiority—well-designed functionality, an intelligent architectural design and support for industry standards.

Unified solutions for endpoint management success
When you evaluate solutions to meet your goals, you will find that IBM offers not only a best-of-breed endpoint management solution, but also extraordinary breadth and integration across a robust security portfolio. IBM solutions are built to provide visibility into your organization's endpoint environment. They can help control the cost of management, security and compliance. And they can help reduce the complexity of managing a heterogeneous endpoint, operating system and application infrastructure.

The saying that "you can't manage what you can't see" is as true in endpoint management as it is anywhere else. Across all functions, the unified visibility and control made possible by IBM endpoint management is designed to break down IT silos that prevent effective, timely endpoint management. Automation and consolidation of tasks, combined with an intelligent agent that continuously and asynchronously manages assessment and policy enforcement, means that a large management server infrastructure is not necessary.

The IBM® Tivoli® Endpoint Manager solution can dramatically shrink gaps in management capabilities and security exposures by quickly and accurately effecting changes across the infrastructure. Built on BigFix® technology, this solution can help reduce security risks, management costs and management complexity as it increases the speed and accuracy of endpoint policy enforcement and remediation. The single agent, single console and single management server approach is designed to increase reliability and deliver rapid time to value through functions such as patch management, configuration management and endpoint discovery. This approach can enhance ROI by increasing operational efficiencies, enabling management infrastructure consolidation and improving IT productivity.

The single-agent approach provided by Tivoli Endpoint Manager further enables organizations to get the most from their current assets. Since the solution's management server is always kept up-to-date by the agent, there is no need to run lengthy scans, execute queries or worry about systems that are shut down or roaming off the corporate network. The agent's autonomous operation, coupled with the visibility provided by a single console, enables administrators to see events taking place across the entire network.

IBM Tivoli Endpoint Manager is part of the comprehensive IBM security and management portfolio, helping organizations address the challenges of a distributed infrastructure. In a smarter planet's instrumented, interconnected and intelligent IT operations, IBM security and management solutions are designed to ensure real-time visibility, centralized control and advanced automation for the entire IT infrastructure, including globally distributed endpoints.

For more information

To learn more about IBM Tivoli Endpoint Manager, contact your IBM 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.

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

© Copyright IBM Corporation 2012

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

Produced in the United States of America
January 2012

IBM, the IBM logo, ibm.com, 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

BigFix is a registered trademark of BigFix, Inc., an IBM Company.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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.

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

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 (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, and so on) 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.

TIO14008-USEN-01