Smarter, faster endpoint management through automation and innovation

IBM Tivoli Endpoint Manager answers your endpoint challenges quickly and accurately

Contents

Introduction

Because IT administrators have access to data that is typically unavailable to other departments, they are often perceived as the "keepers" of intelligence in an enterprise. As such, they are constantly asked questions they did not foresee when they purchased a particular tool—questions that may not fit into discernible categories. Now more than ever, IT administrators must know the answers to these questions, or be able to find the answers quickly. Through the power of IBM Tivoli® Endpoint Manager, built on BigFix® technology, administrators can provide accurate answers to virtually any endpoint question and always stay a step ahead.

Tivoli Endpoint Manager's unique approach distributes intelligence down to the endpoint, giving IT administrators the power to ask the right questions to every endpoint and receive quick, accurate answers. The solution anticipates, assesses, and remediates in real time, giving IT organizations the efficiency and accuracy they need through a single, policy-driven agent and a single console.

Tivoli Endpoint Manager's patented technology distributes computing power to the endpoints themselves, using the intelligent agent to provide a level of visibility and control not possible in legacy solutions. This level of innovation translates into significant advantages in speed, flexibility, and scalability, while reducing the infrastructure and training costs associated with traditional systems and security management.

"For the General Services Administration (GSA), use of Tivoli Endpoint Manager for Power Management on 15,000 machines projects savings of $750,000 annually."

—Doug Beizer, *Federal Computer Week*

Reaping the benefits of distributed intelligence

By pushing intelligence to the endpoint, rather than waiting for an overloaded, centralized server or server farm to process data, organizations can achieve a number of distinct operational benefits. Some of these include:

- A quieter help desk. Well-maintained computers suffer fewer outages, security issues, and other trouble ticket-generating events than poorly maintained ones. This results in a reduced demand for help desk services, reducing costs and freeing technicians to work on other projects.
- Reduced overtime and weekend work. The high reliability of remediation and system management processes reduces the need to schedule these actions after normal working hours or on holidays, significantly cutting overtime costs.
- Increased employee productivity. Many organizations rely on the voluntary efforts of end users to perform at least some maintenance and other administrative tasks on their own computers. The time involved may seem trivial, but can easily add up to tens of hours a year per employee. Remediation actions executed by non-technical personnel also tend to suffer low success rates and generate a higher-than-normal number of trouble tickets. Giving IT the ability to define endpoint remediation policies, many of which execute transparently to the end user, eliminates many of these issues.

Why it works

Critical success factors of Tivoli Endpoint Manager's technology include:

- **A flexible, intelligent agent**—A single agent that uses two percent of CPU on average, and low network impact means its processes are virtually imperceptible by the user. The Tivoli Endpoint Manager agent is capable of assessing the state of the endpoint against policy and bringing the endpoint back into compliance with policy—without any instruction from the management server. This is true of all Tivoli Endpoint Manager's security and systems management functions, from security configuration management to software patch distribution—a single agent is all that is necessary. Regardless of what capabilities you use, there is always a single agent deployed. That means fewer resources required on the endpoint and greater flexibility for solving a wide variety of problems.

- **Instant answers**—Whether it's finding out how many instances of Adobe® Acrobat are installed or validating which laptops are impacted by the latest zero-day threat, Tivoli Endpoint Manager provides answers within minutes across the entire organization. Thanks to the intelligent agent, there is no need to wait for a lengthy scan to complete, a centralized server to churn on the details, or a SQL query to finish running. Each agent evaluates the relevance of the question, analyzes the information, reports back, and even takes action based on that analysis if required.

- **Coverage for roaming endpoints**—Users are connecting to the corporate network from home, hotels, airports, and even airplanes. Always staying a step ahead, Tivoli Endpoint Manager provides the unique ability to manage roaming endpoints in real time at scale—without compromising security—regardless of whether endpoints are located in a corporate office or a coffee shop in Sri Lanka.

How customers are using it

The distributed power of Tivoli Endpoint Manager allows customers around the world to use the solution in many innovative ways. A few examples are provided here.

Imprinting property sticker directly onto the BIOS—on thousands of endpoints in minutes

A Tivoli Endpoint Manager customer gets a large shipment of computers from Dell with property stickers imprinted before the computers are shipped. In another shipment, this information was imprinted onto the flash BIOS, creating inconsistency in the customer's IT asset management processes.

- Customer question: How do we use Dell's asset stamper utility to automatically correlate the asset number to the machine?
- Tivoli Endpoint Manager solution: Dell shipped the customer a spreadsheet listing the machines and the stickers. Tivoli Endpoint Manager populated that list out to the endpoint agents, which matched the serial numbers to the stickers and imprinted the numbers directly onto the BIOS—saving hours of manual input time.
- End result: The solution eliminated the need for IT personnel to spend half an hour correlating devices and property numbers for each of over 8,000 endpoints, resulting in cost savings of over $200,000.

Bringing "off lease" laptops back to HQ

By informing users of approaching lease cycle expiration, one customer saves money by reducing the numbers of "off lease" laptops, facilitating the hardware refresh cycle, and enabling users to be part of the solution.

- Customer question: How do we keep track of all laptops and their lease expiration cycles when our users are so widely distributed?
- Tivoli Endpoint Manager solution: Use Tivoli Endpoint Manager's distributed intelligent agent architecture to pop up a message on the user's screen that the lease cycle has ended, with instructions on how to return the equipment and receive a replacement.
- End result: Before implementing the Tivoli Endpoint Manager solution, the customer was losing over 20 percent of their recalled laptops per year. Based on their laptop population, using Tivoli Endpoint Manager to improve and automate the laptop recall process resulted in cost savings of approximately $3 million.

Using endpoints to troubleshoot network issues

Trying to determine the source of a network issue is not always straightforward. This is particularly true with widely distributed networks that use a variety of connection technologies. A Tivoli Endpoint Manager customer decided to leverage agent intelligence to provide greater visibility into network-related issues. Using the instant visibility from a desktop perspective helps shed light on what is going on in their network in real time—without impacting user productivity.

- Customer question: How can we better triage and troubleshoot network issues using the existing infrastructure?
- Tivoli Endpoint Manager solution: Create a task to retrieve network traces from endpoints and pinpoint specific network issues by evaluating network trace "snapshots" received from them, rather than attempting to gain remote access to those endpoints and impacting user productivity.
- End result: The help desk has achieved better efficiency, using precise and accurate information in real time, without adding any additional infrastructure or network forensics tools and without impacting end-user productivity.

Automatically collecting documents to support e-discovery

As part of an e-discovery litigation procedure, a Tivoli Endpoint Manager customer in the pharmaceutical industry needed to collect all files from the "My Documents" folder of every user's computer in every site around the world. The collection process needed to be performed without user knowledge or interaction, and without impacting network availability or performance—even for remote and roaming laptops.

- Customer question: How can we collect all documents using our existing IT infrastructure, without impacting users, and within a very short timeframe?
- Tivoli Endpoint Manager solution: The IT administrator used Tivoli Endpoint Manager to target specific endpoints and created a task to copy the "My Documents" folder and all of its contents back to a centralized file server. In less than eight weeks, the organization was able to capture all necessary files in "stealth mode," avoiding the need to invest in an e-discovery point product. Thanks to Tivoli Endpoint Manager's dynamic and policy-based bandwidth throttling capability, network service quality was unaffected throughout the process.
- End result: With Tivoli Endpoint Manager, the e-discovery process was fast, accurate, and transparent to the end user. Rather than spending millions of dollars and months of work purchasing and deploying a separate tool, they leveraged the power of the Tivoli Endpoint Manager solution for rapid, cost-effective results.

Monitoring boot-up performance and managing user expectations

There are two common behaviors for end users in enterprise networks. First, users are very demanding when it comes to computer performance, and quickly complain at the first sight of performance degradation. Second, users tend to install unnecessary and non-business related applications on their corporate-owned desktops and laptops, which can cause the very degradation in performance they are trying to avoid, not to mention potentially introducing viruses and other malware into the corporate environment. A Tivoli Endpoint Manager customer in the SaaS industry found a way to solve both problems by implementing a "boot-up performance monitor." This application shows the impact of user-installed software on the boot-up process and provides "click-here" instructions on how to improve performance. Boot-up performance complaints went away—without a single help desk ticket.

- Customer question: How can we respond to users' complaints about computer boot-up performance when we're not sure what applications they've installed (business-related or not)?
- Tivoli Endpoint Manager solution: By using the Tivoli Endpoint Manager client user interface, the IT staff gives users the ability to monitor their own workstation boot-up performance. Additionally, users are given diagnostic information and easy-to-follow instructions on improving boot-up times, such as by removing CPU-intensive programs that are not business-critical.
- End result: The staff has found the perfect balance of delivering quality service to the end-user community without investing in more help desk systems and processes. Additionally, end users are encouraged to remove unnecessary applications, many of which can contribute to network noise, system vulnerabilities and poor workstation performance.

Pushing data to endpoints

Enterprises are more widely distributed today than ever, making systems management tasks like distributing software and patches extremely challenging. Tivoli Endpoint Manager customers are always inventing new, creative ways to leverage the solution beyond these classic applications, however, immediately delivering other types of business-critical data to endpoints. Here are a few examples:

- A gas station company in Asia uses Tivoli Endpoint Manager to quickly distribute pricing data whenever there are changes made to prices at the pumping stations.
- In Singapore, a bank uses Tivoli Endpoint Manager to distribute new images to their ATM machines.
- In Malaysia, a customer uses Tivoli Endpoint Manager to send an action that displays a message to every user every Friday that reminds them to put on traditional attire.
- A large U.S.-based hotel chain uses Tivoli Endpoint Manager to push new prices to reservations centers. With other solutions, it took more than seven days to transfer files, a process that now takes only minutes.

Browser configuration checking for fine-tuned patch targeting

A global telecommunications provider wanted to avoid a blanket "push and pray" approach to patching systems for a specific ActiveX vulnerability. The IT staff wanted to eliminate those systems from the patching cycle that did not have the specific vulnerable configuration. Unfortunately, most patch tools do not have the ability to dig deep into the configuration of a specific application and use that information for targeting purposes—or they may take days to return the required data. Thanks to Tivoli Endpoint Manager's distributed intelligence, detailed information about specific computer properties is easily found within minutes—through a simple query.

- Customer question: How do we validate something so granular as the presence of an ActiveX misconfiguration across 150,000 remote and roaming systems?
- Tivoli Endpoint Manager solution: Tivoli Endpoint Manager's intelligent agent sees all and reports all—on thousands of properties—across a broad spectrum of platforms and third-party applications—in minutes. By issuing a query, the staff received the necessary information across their entire 150,000 endpoints in less than 90 minutes. Other approaches would have taken days to receive results and likely been incomplete.
- End result: By saving time during the asset identification process, the IT staff was able to push out the necessary patch a full week faster than they were able to prior to using Tivoli Endpoint Manager. They were also able to achieve a 98+ percent first-pass success rate for the patch installation, thanks to more effective targeting on the front end.

Tracking down USB devices that "walk away"

USB devices are ubiquitous and very handy for quick file transfers. Unfortunately, it is extremely difficult—if not impossible—to track their usage and location, and harder still when so many are misappropriated by employees and contractors. A retailer used Tivoli Endpoint Manager to track the serial numbers of all USB devices in the environment, as well as where they were last plugged in, and correlated that information with the users logged into each system.

- Customer question: How do we control and track usage of USB devices in order to keep costs down and reduce the risk of data loss exposures?
- Tivoli Endpoint Manager solution: Since the agent has access to (and can report on) thousands of computer properties, including third-party peripheral devices, it is very straightforward to create an analysis and receive results back within minutes. Additionally, Tivoli Endpoint Manager's policy-based management console provides the ability to enforce USB access based on variables (or combinations of variables) such as serial number, user, IP address of the system, or time of day.
- End result: With this level of real-time visibility and control, the retailer was able to track usage of USB devices, saving money and reducing risk at the same time.

Enforcing state-endorsed "no sales tax" holidays on POS terminals

Many states offer a no-tax holiday that requires retailers to stop collecting sales tax during one weekend each year. While this is a positive event for both retailers and consumers, it wreaks havoc on IT staff who must handle these exceptions across their terminals, across different state tax "holidays" and tax calculations. A large retailer doing business across the U.S. uses Tivoli Endpoint Manager to update state tax configuration data on 7,000 POS systems the evening before the holiday, and then automatically switches back to the appropriate tax table at the close of the weekend.

- Customer question: How can I verify that the tax configuration data is being appropriately enforced on the applicable POS devices, across multiple states, on different dates, and in different time zones?
- Tivoli Endpoint Manager solution: As a distributed intelligence solution, Tivoli Endpoint Manager is the ideal choice for this particular use case. It provides the ability to verify that the appropriate changes are made, which is a critical step for ensuring revenue as well as proper tax accounting and auditing.
- End result: Thanks to Tivoli Endpoint Manager's ability to quickly assess, enforce, and validate change in minutes across the POS environment, the retailer was able to ensure no loss of revenue after the tax holiday (and no penalties from incorrectly taxing customers during the holiday). Before Tivoli Endpoint Manager, the retailer learned—months after the tax holiday—that many of the terminals had not been reconfigured to collect tax, resulting in losses of hundreds of thousands of dollars.

Providing zero-day malware protection

Despite the evolution and proliferation of endpoint security products, organizations continue to struggle to protect themselves against malicious code outbreaks. Zero-day malware attacks are an example of risks that are extremely difficult to predict and prevent. One Tivoli Endpoint Manager state government customer was in the difficult position of dealing with a malware outbreak, during which anti-virus vendors had not published updated signatures. As a defensive measure, they needed to quarantine each infected system to slow the spread of the infection and provide time to research the best remediation approach.

- Customer question: What additional layers of protection can we provide in case of zero-day malware infections?
- Tivoli Endpoint Manager solution: Thanks to Tivoli Endpoint Manager's ability to discover anomalous behavior in real time, when faced again with a similar situation, the administrator immediately identified the progress of the infection, targeting the 4,000 affected systems in minutes. In order to protect the rest of the network, the administrator quickly created a Tivoli Endpoint Manager policy that instructed agents on the affected endpoints to block outbound communications on all ports except the management port, automatically quarantining infected endpoints while keeping them accessible for remediation and reconfiguration.
- End result: Tivoli Endpoint Manager's intelligent agent technology provides multiple layers of security to protect against the most sophisticated, rapidly moving and blended threats. This is the single best way to prevent exposure to malicious outbreaks like Conficker and Stuxnet, which exploit systems through a blended mix of risk vectors.

How it works

Tivoli Endpoint Manager offers centralized administration, complete automation, real-time visibility into remediation processes, and the flexibility to solve challenges that IT organizations face now and in the future. By using one Tivoli Endpoint Manager toolset and one unified infrastructure, IT organizations can reduce management complexity and improve productivity, service, and coverage. Tivoli Endpoint Manager delivers this improved productivity and service while providing the added benefit of reducing costs and allowing IT to become proactive rather than reactive.

Continuously assessing the endpoint and enforcing policy—regardless of connectivity—the single, multipurpose Tivoli Endpoint Manager agent represents a radical departure from legacy client-server architectures, powering a resilient distributed intelligent infrastructure. Because the lightweight agent uses two percent CPU on average, it imposes a minimal footprint on the system, negating performance concerns and challenges posed by competitive architectures and solutions.

Tivoli Endpoint Manager can help dramatically lower the cost of operations. Hardware investment is minimal, and substantial time savings are realized from centralizing and automating software updates and configuration updates. With scalability that ranges from one thousand to hundreds of thousands of endpoint systems, Tivoli Endpoint Manager provides critical visibility and control functions for organizations of almost any size.

IBM Tivoli Endpoint Manager is a family of products that all operate from the same console, management server and single intelligent agent. This approach helps you consolidate tools, reduce the number of endpoint agents, and reduce management costs. Adding more services is a simple matter of a license key change—no additional software or hardware is required. 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

Tivoli Endpoint Manager is part of a comprehensive Tivoli security and automation portfolio, helping organizations address challenges for users and identities, data and information, applications and processes, networks, and servers and endpoints. Facilitating the instrumented, interconnected and intelligent IT operations of a smarter planet, IBM Tivoli 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 the IBM Tivoli Endpoint Manager family of products, 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.