



BigFix Endpoint Management

Providing Answers to Questions You Didn't Know You Had

Because IT administrators have access to data that's typically unavailable to other departments, they are often perceived as the secret “keepers” of intelligence in an enterprise. As such, they are constantly asked questions they didn't foresee when they purchased a particular tool—questions that may not fit into discernible categories. Yet now more than ever, IT must know the answers to these questions, or be able to find the right answer quickly. Through the power of the BigFix Endpoint Management Platform, IT administrators can provide accurate answers to virtually any question and always stay a step ahead.

“For the General Services Administration (GSA), use of BigFix Power Management on 15,000 machines projects savings of \$750,000 annually.”

Doug Beizer
“Agencies Can Get Power Management Software”
Federal Computer Week Online

Distributed intelligence is about economizing processes through efficiency. BigFix’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 without having to script extensive SQL queries. BigFix anticipates, assesses, and remediates in real-time, giving IT the efficiency and accuracy they need through a single, policy-driven agent and single console.

BigFix’s patented technology distributes computing power to the devices themselves, using the intelligent BigFix 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.

Why It Works

Critical success factors of BigFix’s technology include:

- **A Flexible, Intelligent Agent**—A single agent uses less than 2% of CPU on average and low network impact means its processes are virtually imperceptible by the user. The BigFix 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 BigFix’s security and systems management applications—from security configuration management to software distribution—a single agent is all that’s necessary. So regardless of what specific solution you use, there will always be one single agent that’s deployed. That means less resources on the endpoint and greater flexibility for IT trying to solve a wide variety of problems.
- **Instant Answers**—Whether it’s finding out how many instances of Adobe Acrobat are installed or validating which laptops might be impacted by a manufacturer recall, BigFix provides answers within minutes—across the organization. Thanks to the intelligent agent, there’s 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 can evaluate the question as relevant on its own, analyze, report back and even take an action based on that analysis if desired.
- **Coverage for Roaming Endpoints**—The corporate-owned laptop has moved well beyond the confines of a corporate office. Users are connecting from home, hotels, airports, etc. Always staying a step ahead, the BigFix platform gives IT the unique ability to manage their endpoints in real-time at scale—even for roaming laptops.

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, the IT staff achieves a number of distinct procedural benefits. Some of these include:

- **Quiet help desk.** Well-maintained computers suffer fewer outages, security issues, and other trouble ticket-generating events than poorly maintained machines.
 - **Result:** Reduced demand for help desk services, either in-house or outsourced.
- **Reduced overtime and weekend work.** The high reliability of BigFix remediation and system management processes reduces the need to schedule these actions after normal working hours or on holidays, significantly cutting overtime costs.
- **Undistracted non-technical employees.** Many organizations rely on the voluntary efforts of end users to perform at least some maintenance and other administrative tasks on their computers. The time involved may seem trivial, but can easily add up to several hours a year per employee. Also, non-expert-executed remediation actions tend to suffer low first-pass success rates and generate a higher-than-normal number of trouble tickets.

How Customers Are Using It

The distributed power of the platform is allowing customers globally to use BigFix in the following innovative ways:

Imprint Property Sticker Directly Onto BIOS—on thousands of endpoints in minutes.

One customer gets their computers from Dell, with a property sticker before they are shipped. In one shipment, this information was imprinted onto the flash BIOS. But not all systems were being shipped this way.

- **Customer question:** How do we use Dell’s asset stamper utility to automatically correlate the number to the machine?
- **BigFix solution:** Dell shipped BigFix a spreadsheet containing machines and the stickers—they populated that list out of the endpoint. BigFix matched the serial number to the sticker and imprinted the number directly onto the BIOS—saving the customer hours of manual input time.
- **End result:** With 8–9K endpoints and about 30 minutes per laptop, the customer saved 4000 hours of tech time at \$45–60/hour.

Bring “Off Lease” Laptops Back to HQ

By informing users of approaching lease cycle expiration, one BigFix customer saves money by reducing the numbers of “off lease” laptops, facilitating the hardware refresh cycle and helping users 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?
- **BigFix solution:** Use BigFix’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 BigFix solution, the customer was losing over 20% of their recalled laptops per year. Based on their laptop population, using BigFix to improve and automate the laptop recall process resulted in approximately \$3MM of savings.

Use 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 using a variety of different connection technologies. A BigFix 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’s 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?
- **BigFix solution:** Create a task to retrieve network traces from endpoints and pinpoint specific network issues by evaluating network trace “snapshots” from them, rather than attempting to gain remote access of those endpoints and impacting user productivity.

With BigFix, e-discovery 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, the customer leveraged the power of the BigFix platform for rapid, cost-effective results.

- **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.

Automatically Collect Documents to Support E-Discovery

As part of an e-discovery litigation procedure, a BigFix 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 as well as not impact 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, within a very short timeframe?
- **BigFix solution:** The BigFix operator targeted a specific group of users and created a task to copy the “My Documents” folder and all of its contents back to a centralized file server. Within 6–8 weeks, they captured all necessary files in “stealth mode”, avoiding the need to invest in an “e-discovery” point product. Thanks to BigFix’s dynamic and policy-based bandwidth throttling capability, network QoS was unaffected throughout the process.
- **End result:** With BigFix, 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 BigFix platform for rapid, cost-effective results.

Boot-Up Performance Monitoring and Managing User’s Expectations

There are two common behaviors for end-users in enterprise networks. Firstly, when possible, users will inevitably install unnecessary and non-business related applications on their corporate-owned and managed desktops and laptops. Secondly, they will often complain at the slightest perception of computer performance degradation. A BigFix customer in the SaaS industry found a way to solve both problems—by implementing a “boot-up performance monitor” that showed the impact of user-installed software on the boot-up process and providing “click-here” instructions on how to improve performance. Users complaints went away—without a single helpdesk ticket.

- **Customer question:** How can we respond to a user’s complaint that their computer boot-up performance is lagging when we’re not sure about every application they’ve installed (business-related or not)?
- **BigFix solution:** By using the optional BigFix Client UI, 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. For example, by removing CPU-intensive programs that aren’t business-critical.
- **End result:** The IT staff has found the perfect balance of delivering quality service to the end-user community without investing in more helpdesk 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 than ever before—making systems management tasks like distributing software and patches extremely challenging. However, there are other more esoteric pieces of payload that BigFix customers need to get to endpoints immediately. Here are a few examples:

- A gas station company in Asia uses BigFix to quickly distribute pricing data whenever there are changes made to prices at the pumping stations
- In Singapore, a bank uses BigFix to distribute new images to their ATM computers.
- In Malaysia, a customer sends an action that invokes a flash message to every user each Friday that reminds them to put on their traditional attire.
- A large US-based hotel chain uses BigFix to push new prices to reservations centers. With other solutions, it took over 7 days to transfer files which now happens in minutes with BigFix.

IE 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. IT staff wanted to eliminate those systems from the patching cycle that didn’t have the specific vulnerable ActiveX configuration. Unfortunately, most patch tools don’t have the ability to dig deep into the configuration of a specific application and use that information for targeting purposes. Thanks to BigFix’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—particularly across 150,000 remote and roaming systems?
- **BigFix solution:** BigFix’s intelligent agent sees all, and reports all—on thousands of properties—across a broad spectrum of platforms and third-party applications. By issuing the query via a BigFix “Fixlet”, the IT staff received the necessary information across their entire 150,000 endpoints within less than 90 minutes. Other alternatives would have taken days to receive results.
- **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 BigFix. They were also able to achieve a 98%+ first pass success rate for the patch installation thanks to more effective targeting on the front end.

Track Down USB Devices That “Walk Away”

USB devices are ubiquitous and quite handy for quick file transfers. Unfortunately, it is extremely difficult—if not impossible—to track their usage and location, and worse still when so many are stolen by employees and contractors. A retailer used the BigFix platform to track serial numbers of all USB devices in the environment, where they were last plugged in, and correlated that 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?
- **BigFix solution:** Since the BigFix Agent has access to (and can report on) thousands of computer properties, including third party peripheral devices, it is very straightforward to simply create an analysis, and receive results back within minutes. Additionally, BigFix’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.

BigFix intelligent agent technology provides multiple layers of security to protect against the most sophisticated, rapidly-moving and blended threats.

Enforcing State-Endorsed “No Sales Tax” Holidays on POS Terminals

Many states offer a no-tax holiday that allows retailers to avoid charging or collecting sales tax during one weekend each year. While this is a happy event for both retailers and consumers, it wreaks havoc on the IT staff to handle these exceptions across their POS terminals, with different state “holidays” and tax calculations. A large retailer doing business across the US uses BigFix to enforce data on the 7,000 POS systems from a state tax record configuration table the evening before the holiday, and then automatically switches back to the appropriate tax value 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 states, on different dates and time zones?
- **BigFix solution:** Since BigFix is the industry’s only distributed intelligence solution, it was the best choice for this particular use case. Alternative solutions don’t have the ability to verify these changes are made, a critical step for proper tax accounting and auditing, and revenue.
- **End result:** Thanks to BigFix’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. Before BigFix, the retailer learned that months after the tax holiday, many of the POS terminals hadn’t been reconfigured to collect tax, resulting in losses of hundreds of thousands of dollars in some cases.

Zero Day Malware Protection

Despite the evolution and proliferation of endpoint security products, organizations continue to struggle to protect against malicious code outbreaks. Zero day malware is one example of a risk that is extremely difficult to predict and prevent. One BigFix state government customer was in the difficult position of having a malware outbreak for which the existing AV vendor didn’t yet have an updated signature. They used BigFix to automatically quarantine each infected system to slow the spread of the infection and to give time to figure out the best way to remediate.

- **Customer question:** What additional layers of protection do we have in case of a zero day malware infection?
- **BigFix solution:** Thanks to BigFix’s ability to discover anomalous behavior in real-time, the administrator immediately identified the progress of the infection and targeted those 4,000 systems that were affected. In order to protect the rest of the network, the BigFix Agent enforced a block on outbound communications on all ports except the management port. The infected machines were quarantined and yet still accessible for remediation and reconfiguration.
- **End result:** BigFix 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, which exploit systems through a blended mix of risk vectors.

BigFix can dramatically lower the costs of IT operations. Hardware investment is minimal, with substantial time-savings from centralized automation of software updates.

How it Works—BigFix Endpoint Management

BigFix 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 BigFix toolset and one unified infrastructure, IT staff can reduce management complexity and improve productivity, service, and coverage. BigFix offers this improved productivity and service while providing the added benefit of reduced costs.

Laying the foundation of the BigFix solution is the BigFix Endpoint Management Platform, which comprises the BigFix Agent, BigFix Server, BigFix Policy Messages, and BigFix Relays.

Continuously assessing the endpoint and enforcing policy—regardless of connectivity—the single, multi-purpose BigFix Agent represents a radical departure from legacy client-server architectures and powers a resilient distributed intelligent infrastructure. Because the lightweight BigFix Agent uses <2% CPU on average, it imposes a minimal footprint on the system, avoiding performance concerns and challenges posed by legacy architectures and solutions.

The BigFix Agent communicates policy information with the BigFix Server—which hosts the BigFix console, reporting/analysis dashboards, and policies—through BigFix Policy Messages, also known as “Fixlet” messages. BigFix Relays act as communication and aggregation points and staging areas for BigFix Policy Messages and patch/remediation content.

BigFix can dramatically lower the costs of IT operations. Hardware investment is minimal, with substantial time-savings from centralized automation of software updates. With scalability that ranges from one thousand to hundreds of thousands of endpoint systems, BigFix can provide critical visibility and control functions for organizations of almost any size. Configuring the ideal mix of BigFix products can help IT organizations lower costs and improve services, while maintaining a high level of commitment to services delivery.



BigFix: Breakthrough Technology, Revolutionary Economics

Founded in 1997, BigFix, an IBM Company, is a leading provider of high-performance enterprise systems and security management solutions that revolutionizes the way IT organizations manage and secure their computing infrastructures. Based on a unique architecture that distributes management intelligence directly to the computing devices themselves, BigFix is radically faster, scalable, more accurate and adaptive than legacy management software. From Systems Lifecycle Management, Security & Vulnerability Management to Endpoint Protection, BigFix solutions automate the most labor-intensive IT tasks across the most complex global networks saving organizations significant amounts of time, labor, and expense. BigFix provides real-time visibility and control for millions of globally distributed computing devices. The BigFix customer list counts many of the world's largest and most prestigious organizations in every industry including financial services, retail, education, manufacturing, and public sector agencies. More information can be found at www.bigfix.com

©2010 BigFix, an IBM Company. BigFix and the BigFix Logo are registered trademarks of BigFix, an IBM Company. Other trademarks, registered trademarks, and service marks are property of their respective owners.
20100903