

# WHITE PAPER



## **BIGFIX: REAL-TIME, PERVASIVE AND DEEP ASSET DISCOVERY**

*By Amrit Williams, Chief Technology Officer, BigFix, Inc.*

BigFix's approach to IT infrastructure asset discovery, by combining real-time situational awareness of device configuration and pervasive coverage of virtually all assets of management concern is nothing short of revolutionary. These attributes, unique to BigFix, transform asset discovery from a static, "bean counting" snapshot exercise to an enabling function for dynamic, in-the-moment management of IT assets and the value they deliver to their host organizations.

## Picture Window Into the Infrastructure

The BigFix single-agent/single infrastructure architecture enables pervasive discovery and management of data center, desktop and mobile computers. BigFix is not just a Windows-only solution. The BigFix Agent runs on all versions of Microsoft Windows since Windows 95 as well as popular flavors of Unix, Linux and Mac OS. BigFix can help IT organizations maintain visibility into mobile laptop and notebook computers, even when roaming beyond the immediate confines of an enterprise network. Here, the BigFix Agent not only runs on mobile computers, but the BigFix Platform includes mechanisms for secure communications to BigFix Consoles over the Internet and other wide-area connections. This creates a consolidated view of computing assets regardless of their hardware and software platforms.

Furthermore, BigFix can recognize and provide information on any IP-enabled device through BigFix's unique distributed scanning technology. This latter class of devices includes network peripherals and plumbing such as printers, scanners, routers, switches and so on. While these devices may not be completely manageable through BigFix, customers can see them and evaluate their impacts on infrastructure operations.

The pervasiveness of BigFix reduces blind spots and increases the pool of manageable assets. On installing BigFix, customers often discover to their surprise that their organization owns significantly more computers—usually in the 20-30 percent range—than they had previously inventoried. At this point, customers can decide to bring this previously dark matter under management, or eliminate it as surplus to requirements.

## In-the-Now Situational Awareness

Real-time information on asset configurations and assets creates a state of dynamic situational awareness about what's going on in the IT infrastructure. This contrasts to traditional asset discovery, which tends to be just that, a sporadic Easter egg hunt resulting in static snapshots that fail to capture fast changing conditions. In a very real sense, having real-time visibility is the difference between driving a car aided by instant photographs taken through the front window every 10 minutes, and seeing the road through an unobstructed windshield.

### Running Ahead of Anti-Virus Tools

An electric utility in the Southern US uses BigFix to report anomalous behavior in managed devices that could indicate infections by viruses and other malware. The company can then write a Fixlet message to block execution of the malicious execution thread and propagate this remediation throughout their infrastructure. BigFix administrators say that in almost every case, their anti-virus software vendor issued a new virus definition file to its users weeks after the BigFix administrators first discovered the virus on their infrastructure.

### Unexpected Overpopulation

A US consumer financial company installed a license to manage what they thought was a population of 50,000 desktop computers. BigFix reported that the organization actually hosted some 80,000 machines. Subsequent investigation proved that the BigFix-reported figure was correct. The organization used this information to reduce its surplus computers and bring the remainder under active management.

Sampling rate theory applies in the case of static asset discovery. To know what is going on in a period of time, you need to sample a given phenomenon twice as fast as its maximum rate of change. This is why CD-quality digital recorders sample sound 44,000 times a second, twice the rate of a 20,000 Hertz high frequency audio signal. In the IT world, doing an asset inventory every week will tell you what is going on in an asset base to a resolution of two weeks. This is clearly unacceptable in today's high velocity threat environment where viruses can spread in minutes and intruders and sensitive data can leak in seconds and lead to a lifetime of regret.

BigFix goes deep to report all relevant information about an asset's status and configuration up to the BigFix Console. This provides not only a powerful tool for compliance reporting, but can also translate into real-time decision support when processed via correlation and analysis tools. Information depth also applies to non-BigFix Agent equipped devices. Again, while lack of an installed BigFix Agent on these devices may preclude their active management, information returned from them can be valuable in maintaining secure and efficient infrastructure operations.

BigFix solutions can scale to deliver these unsurpassed levels of real-time visibility and control on infrastructures up to 200,000 managed endpoints from a single BigFix Server. By relying on managed endpoints to supply the computing resources to run the BigFix Agent, the more endpoints, the more resources available to the overall BigFix solution.

The BigFix Agent itself is very lightweight, ranging between 2-4 megabytes of endpoint system memory and consuming 1-2 percent of processor bandwidth when active. The Agent works by sending messages upstream to the BigFix Server when changes occur in a

The screenshot shows the BigFix Enterprise Console interface. The top window displays a list of 115 unmanaged assets, sorted by Asset ID. The list includes columns for Asset ID, Source Name, Hostname, OS, Running Client, Creation Time, and IP Address. Below the list, the 'Unmanaged Asset: 45' summary is shown, including a table of identifying properties.

Property Name	Property Value
Device Type	printer
First Scan Time (Server Time)	9/12/2005 2:00:24 PM
Hostname	n/a
Import Time (Server Time)	1/23/2006 8:39:38 PM
IP Address	10.48.134.73
Last Scan Time (Server Time)	9/12/2005 2:00:24 PM
MAC Address	00:04:00:18:55:AC
Newly Discovered	yes
OS	Lexmark M412n network printer

**BigFix Asset Discovery can supply detailed information on many kinds of unmanaged assets, i.e. those that do not run the BigFix Agent.**

managed device's status or configuration. This resembles data compression techniques used in high definition video technologies. HD video conserves bandwidth and storage requirements by transmitting data about only those pixels that change in a moving television picture. To further conserve system resources and communications bandwidth, BigFix users can set controls to throttle the BigFix Agent or BigFix management communications across a network.

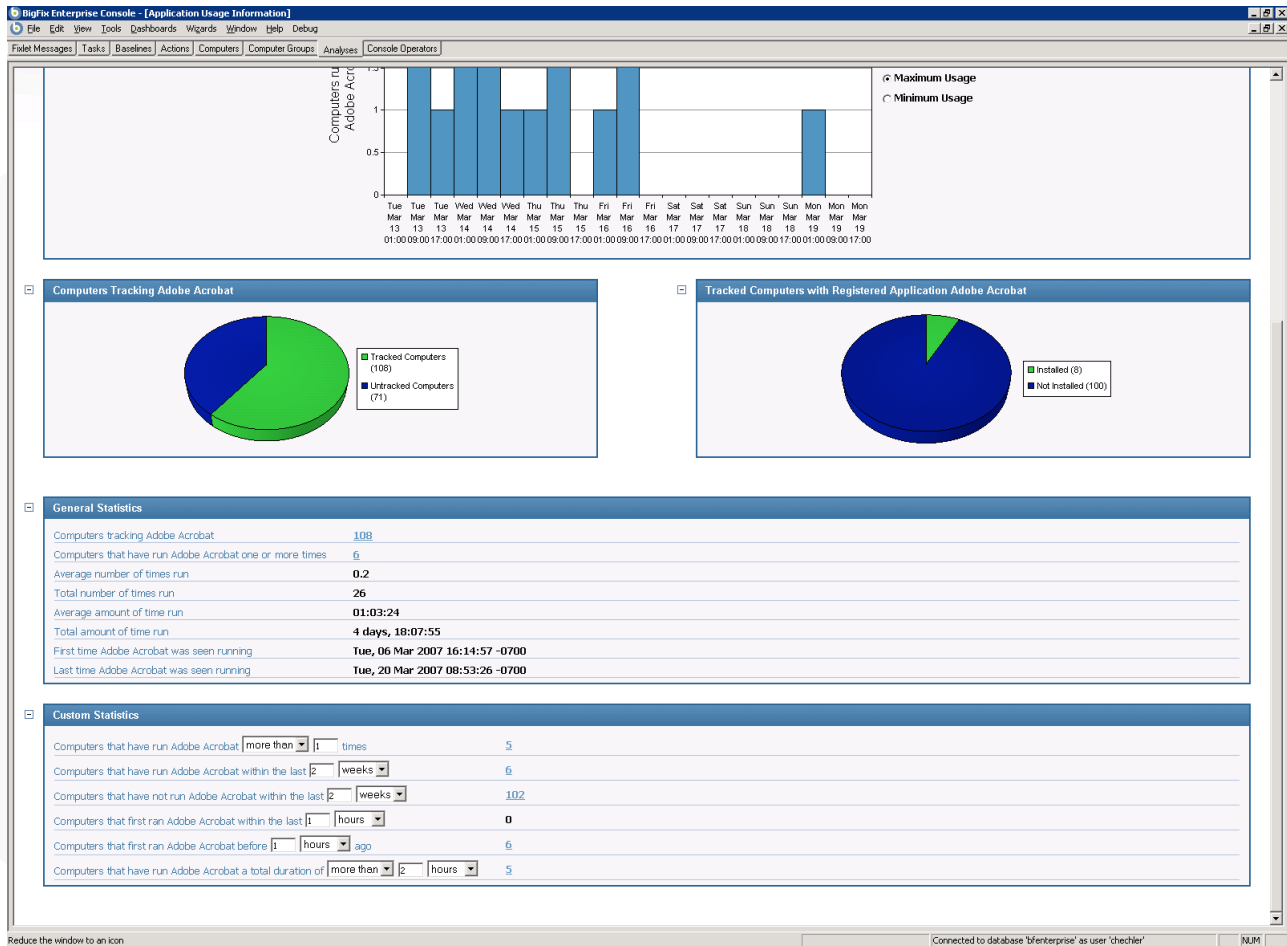
## The Uses of Visibility

Real-time visibility would be little more than a magic trick if it did not radically improve management of IT infrastructures. The pervasiveness, real-time reporting, information depth, scalability, and flexibility of the BigFix technology platform open the floodgates to a series of radical changes in how organizations manage and harvest value from IT infrastructures.

Infrastructure management innovations begin with the ability to integrate BigFix real-time asset discovery and reporting with allied security and system management processes. The growing array of BigFix policy modules, extensions and solution packs consolidate much previously discrete process onto a common, well-understood infrastructure. Customers find that they can reduce the licenses they need for individual, multivendor tool collections. Also, as BigFix-supported visibility and management services span both system management and information security fields, this creates opportunities to integrate and align these heretofore disaggregated process disciplines.

Although BigFix centers on the BigFix Agent, customers frequently reduce the overall number of agents and "tool clutter" on managed endpoints through consolidated service delivery through the BigFix Platform. Consolidating on the BigFix infrastructure also gives IT staffs the opportunity to develop deep expertise in the BigFix solution. As a result, BigFix customers report significant gains in IT service delivery quality, staff productivity, and returns on investment far in excess of costs incurred implementing and operating BigFix-based solutions.

# WHITE PAPER



**BigFix software licence tracking can help organizations cut costs by identifying under-utilized licenses and assuring that software is used most productively.**

## Non-Stop Policy Enforcement

BigFix real-time asset discovery sets the stage for pervasive, timely, and effective security policy enforcement. BigFix operators can see and know when assets log on and log off the network. BigFix solutions can automatically assess endpoints against baselines, and initiate remediation measures where appropriate. This leads to a preemptive approach to security configuration management where maintaining assets against a prescriptive baseline sharply reduces the busy work of after-the-fact patches, vulnerability fixes, and other endpoint micro-management exercises.

A number of BigFix customers have used real-time asset discovery and proactive policy enforcement to implement software-based Network Access Control solutions. These solutions use BigFix policies to assess device conformance against security dress codes. After that, the BigFix solution can admit a device, block it, or remediate it prior to granting network access privileges.

### Software License Reduction ROI

A large telecommunications service provider used BigFix to track usage patterns for expensive SQL server software licenses. It discovered that only 28 of 100 licenses were used by the organization. The company reduced the quantity of licenses it ordered at the next renewal opportunity and save \$1.5 million.

BigFix users can extend policy enforcement to cover mobile laptop/notebook computers. BigFix Agents installed on mobile devices stay in force even when these machines roam off the network. To maintain maximum visibility in these computers, BigFix customers can set up BigFix access points in DMZs outside the organization's network firewall. From there, mobile computers can be instructed to "phone home" to the BigFix solution every time they connect to the Internet.

## Just-in-Time Service Delivery

Real-time asset visibility also enables just-in-time service and application delivery to BigFix managed endpoints. BigFix managed endpoints can signal requests for a service or software up to the BigFix Server and receive an immediate response in the form of a remediation action, software update, application installation or other action. These functions can be scripted to enable fast transfer of software and licenses to endpoints that actually needed to use an application, while uninstalling underutilized software on other machines.

More prosaically, BigFix Asset discovery and license management can help organizations cut software licensing costs by identifying unused “shelfware” licenses and supporting non-penalty-generating conformance to licensing terms and conditions over the life of a contract.

Real-time visibility and control can also lead to establishing an ongoing dialog between IT managers and their infrastructures. BigFix includes wizards and a custom command language that makes it easy and fast to query and correct the infrastructure on an ad-hoc basis. Customers have told us that reporting tasks originally budgeted for weeks of committee work often transact in a few minutes of work by a reasonably well-skilled BigFix operator.

## Flexible and Customizable

BigFix is highly customizable and flexible. The BigFix Fixlet language enables rapid development of custom services. BigFix can also provide a window and control channel for non-BigFix third-party applications. Many customers, for example, prefer to deploy brand-name anti-virus clients, but see and manage them through a BigFix solution. Not only do they find the BigFix visibility and management infrastructure superior to that of third-party vendors, they can consolidate anti-virus services under a common process set.

The array of visibility and management services available through BigFix continues to expand as BigFix, Inc., third-party developers and even individual BigFix users create BigFix-deliverable services and functions. BigFix encourages third parties through its partner program, user group and forum, and user training and certification programs.

## The Bottom Line

Real-time visibility delivered through the BigFix Platform does more than improve IT infrastructure management—it changes it. BigFix sharply reduces the ambiguities, latencies, and opportunities for error, formerly associated with IT asset management. Organizations they can consolidate many previously discrete processes, reduce their costs and improve quality of service.

Organizations experience some of the most profound benefits through the confidence they gain after building knowledge on how to make BigFix work for them. Fear of the unknown subsides as the infrastructure reveals itself to real-time observation. Processes transact faster and more completely with less worry that a routine change might trigger a service outage or other catastrophe. With BigFix, seeing is better than believing—it's doing and knowing.

### Bad Batteries

When Dell Computer announced in the Summer of 2006 that a number of defective batteries had shipped in some of its laptop computers, many organizations asked their employees—many of them non-technical types—to physically inspect their laptops and report serial numbers of potentially dangerous batteries. BigFix quickly developed and distributed a Fixlet message that enabled its customers to automatically search for defective batteries in their infrastructure and transmit results to the BigFix Console. Customers reported that they had accurate information about affected machines within minutes of launching the Fixlet message to BigFix-managed assets.