

## **The BigFix Solution**

By Amrit Williams  
Chief Technical Officer,  
BigFix, Inc.

### **The BigFix Solution**

BigFix was designed not to cope with a world that was expected to come to pass, but to thrive in an unpredictable one. Rather than addressing problems of immediate concern, BigFix set out to build a platform that would create an infrastructure and methodology for problem solving, whatever those problems happened to be. The following more explicitly maps out how BigFix technology changes the traditional enterprise systems management paradigm. BigFix is a massively scalable distributed processing system designed to continuously discover, assess, remediate, and enforce the health and security of distributed enterprise desktop, mobile and server computers in real-time via a single, policy-driven agent. BigFix's patented technology distributes computing power throughout the enterprise using the lightweight, multi-function, intelligent BigFix Agent to provide a level of visibility and control unparalleled in legacy solutions. BigFix offers significant advantages in timeliness, flexibility, and scalability, while reducing the infrastructure and training costs associated with traditional systems and security management. BigFix is a revolutionary technology that will fundamentally change the way IT functions.

### **Distributed Visibility and Management Nervous System**

As noted earlier, BigFix implements a differentiation between the BigFix Core Services Platform and problem space-focused policy libraries. BigFix Core Services—the BigFix Agent, BigFix Server, BigFix Console, BigFix Relays, and BigFix Fixlet messages—instrument a lightweight and dynamic content-driven messaging and management control system that distributes the work of managing IT infrastructures out to the managed devices themselves, enforcing policies set by infrastructure managers and IT stakeholders. This contrasts with traditional client-server management systems that rely on a central server for all information processing. These solutions may employ agents, but in a distinctly subordinate role to central management resources. To execute a typical management action, these solutions perform a series of inventory and query actions and then have to wait for the agents to respond. This puts tremendous load on the network as well as the servers, not to mention the operators who have to force the information refresh. Basically, traditional systems management tools have a big central brain, with many dumb fingers. If the fingers lose connectivity to the brain, they go limp. Worse, devices that are not connected to the network or to the central server at the time of a management action aren't touched at all and become invisible to infrastructure managers. BigFix Agents resident on managed endpoints continuously assess their endpoint against the organization-specific issues that drive IT, regardless whether they are currently

connected to the BigFix Server or not. While BigFix also has a central nervous system with many fingers that span throughout the organization, the fingers also have localized brains. This means BigFix works everywhere, all the time, no matter whether a BigFix managed asset is on or off the network.

### **BigFix Agent**

Every BigFix-managed desktop, mobile, and server computer runs the BigFix Agent that continuously executes policy instructions (BigFix Fixlet messages) sent to it from the BigFix Server. A single BigFix Agent can execute a wide variety of policies, without requiring multiple agents to manage single functions. This reduces tool clutter, administrative hassle and licensing costs. Furthermore, management actions and results report back to the BigFix Console in real-time.

BigFix's end-point intelligence is particularly beneficial when supporting unstructured or ad-hoc queries. When administrators need to ask a new question concerning endpoint configuration states, administrators can either write a custom BigFix Fixlet message or send a pre-packaged Fixlet message from an established BigFix policy library to every BigFix Agent in the infrastructure. This kind of Fixlet message will include information defining the problem and conditions that make an endpoint eligible to suffer from it. The definition includes a computer readable manifest of the properties that must exist for the problem to occur. In responding to the Fixlet message, the Agent analyzes its local state against the property manifest to determine whether it is affected by the problem, and will send a short report to the BigFix Server if the problem exists on that endpoint. Should the problem exist, the Agent can then request remediation content for execution on the endpoint, install the remediation, and then report that the issue has been resolved.

This patented approach to determining where problems exist, in real-time, provides three fundamental advantages. First, by distributing the computational load for management throughout the environment, assessment and remediation transpires in parallel, with each BigFix Agent requiring only a few seconds to examine their local state to determine whether they suffer from a condition or set of conditions. This contrasts to the hours, days, or weeks, required by other systems management tools to scan an infrastructure for symptomatic data for transmission to a server, which then sorts through this data to determine whether certain conditions on a set of machines exist. Second, because endpoint-resident BigFix Agents are continuously evaluating local states, and reporting from the outside in, the server does not need to run queries against all agents to determine whether an asset suffers from a problem. Every endpoint stands up and presents data on the query immediately.

Third, since the agent software locally inspects its own properties, BigFix avoids the need to invest in dedicated network and server capacity that would be required to transfer and store the megabytes of data that support legacy system scan and remediate processes. Also while other systems need to transfer all data

for analysis at the server, BigFix Agents only report if the problem exists at their particular endpoints. As a result, BigFix can provide a real-time view into problems that exist in the environment, rather than wait for returns on issues that were relevant weeks ago. This kind of real-time visibility and control reduces the load on the network infrastructure, the server, and the assets themselves and significantly improves the operational efficiency of IT organizations by shortening and reducing ambiguity of query/remediation actions.

### **BigFix Server and Console**

The BigFix Server is software running on low-cost, off-the-shelf, Microsoft Windows-based hardware that provides the visibility and operations center for BigFix solutions. The BigFix Server acts as a central resource for managing data, policies, and content sent to and received from the BigFix Agents and provides an administrative user interface in the form of the BigFix Console. A single, low-cost, \$5,000-8,000-class x86 machine running the BigFix Server can manage more than 50,000 BigFix Agent-equipped devices. Furthermore, BigFix Server software includes delegation of control features enabling wide leeway to assign management responsibilities to local and domain-expert administrators as necessitated by org chart or other factors.

### **BigFix Fixlet Messages**

BigFix Fixlet messages communicate policy information and instructions to the BigFix Agent. Fixlet messages contain logical criteria stating what conditions need to exist on a device for an action to occur (for example, devices exhibiting a specific condition), programmatic instructions (“if vulnerability X exists on this client, update software module Y”), configuration parameters (update personal firewall to block all ingress traffic to port 445) and executable content (a software application update packaged for installation). Fixlet messages can be supplied to customers as pre-fab, ready-to-run policy content from BigFix or third parties, or written by customers themselves using the BigFix Fixlet Message Relevance language.

The BigFix Fixlet Relevance language is a published command language that enables BigFix customers, partners and developers to create custom policies and services for BigFix managed assets. It can be used to solve common problems experienced by every large enterprise, such as deployment of patches, configuration management, anti-virus management, or software deployment or be used to write on-the-fly inquiries and remediations to manage the every day curve balls and unstructured problems encountered by almost every enterprise IT operation. Although the Fixlet Relevance language is the primary means BigFix uses to distribute policy content to its customers, the language is far from proprietary. BigFix offers training courses in it and encourages its customers and third parties to use it as a lingua franca for security and system management.

## **The BigFix Relay**

BigFix Core Services includes an important mechanism to enable efficient communications across distributed environments-the BigFix Relay. When implementing a BigFix solution, administrators can designate almost any BigFix Agent-managed computer as a BigFix Relay. BigFix Relays reduce network bandwidth demand needed to support BigFix services by providing multiple concentration, distribution, and fault-tolerant communication points for BigFix policy and remediation content and agent communications. Because BigFix Relays do not require dedicated computers to host them and run as shared services in Microsoft Windows environments, end-users can work with BigFix Relay-equipped computers without noticing performance slowdowns or processor/memory overloads. In fact, many end-users are completely unaware if their asset is also providing a relay function in the enterprise.

To enhance management of mobile and remote devices, BigFix Agents support Relay auto-selection. This enables all BigFix managed assets to find any BigFix relay registered to an enterprise, regardless of its location. This offers extremely powerful capabilities, as mobile devices will automatically communicate with the nearest secure BigFix Relay even when not connected to the corporate network or traversing a corporate VPN.

## **BigFix Management of 3<sup>rd</sup> party end-point security technologies**

BigFix Client Manager for End Point Security consolidates multiple security technologies and makes them seamlessly manageable through the BigFix Console and the BigFix Agent. BigFix replaces the complexity, clutter, and expense of multiple, single purpose tools with a unified approach to anti-malware service delivery covering desktop, server and mobile computers, local and remote, on- or off-network. BigFix sets the stage for proactive, preemptive, policy driven anti-malware threat suppression at enterprise scale.

BigFix provides out of the box Enterprise-class management for 3rd party end point security clients enabling organizations to centrally deploy and manage 3rd party security technologies such as McAfee ePO or IBM/ISS Proventia, uninstall and remove out of date or non-compliant applications, distribute updated definitions and configuration files, consolidate and centralize reporting. BigFix enables an organization to verify, in real-time, and across their entire environment that the correct software is installed, running, configured, and up to date.

## **BigFix Payload Distribution**

The BigFix infrastructure lays down the rails for fast, efficient, and pervasive enterprise wide payload distribution. BigFix enables just-in-time service and application delivery to BigFix managed endpoints. BigFix distributes encryption technologies such as those offered by Guardianedge or Mobile Armor, anti-virus software such as McAfee or Symantec, and security management technologies to hundreds of thousands of assets in minutes and hours compared to traditional

methods that can take day, weeks, or even months. BigFix managed endpoints can signal requests for a service or software up to the BigFix server and receive an immediate in the form of a remediation action, software update, application installation or other action.

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.

### **BigFix Network Access Control**

Continuous policy enforcement, the ability to update security defenses, patch systems, and reconfigure devices, on or off the network is critical to moving an organization from reactive, fire-fighting mode to a mature security posture that puts the organization back in control of their systems. This is particularly true with NAC solutions where continuous policy enforcement can be used to assess and “pre-mediate” devices to conform to NAC dress codes before they log onto the network.

Currently, the vast majority of system management solutions do not enable effective continuous policy management. Weaknesses for conventional system management technologies fall into three areas. First, they lack real-time information on managed device configuration state. This is particularly the case for scanning-based solutions where configuration information is only valid at the time of a scan, and a long interval between scans due to the workloads they impose on networks and managed devices. Even if an organization could scan its infrastructure daily for policy compliance, this gives managed devices 24 hours to drift out of compliance, get infected by malware and generally set themselves up as candidates for quarantine.

Second, most conventional solutions have blind spots that exclude significant classes of assets from effective assessment and remediation. For starters, it’s common for many solutions to focus on only a single technology platform—usually Microsoft Windows. While Windows remains the biggest game in town, it’s not the only game. Most organizations will also need to manage Unix and Linux devices and may also need to enable access for technology platforms not officially supported by the organization, but used by qualified outsiders or employees checking in from home or on the road, i.e. Mac OS.

Beyond that, the biggest blind spot for conventional approaches is poor management coverage of mobile laptop/notebook systems. This is perverse as these are the systems that are most likely to regularly request access to enterprise networks, fall out of compliance and pick up malware while roaming. It does not go too far to say that a security and configuration management solution

that does not offer equivalent management service levels to both fixed and mobile assets is useless in supporting NAC solutions.

Third, administrators must use multiple tools to remediate the wide variety of configuration settings and software (both operating systems and applications) that may be subject to a NAC dress code. This not only slows the process of assessing and remediating managed devices, but any additional complexity in technologies and processes creates opportunities for errors and inconsistencies.

BigFix offers consolidated IT security policy management capabilities that overcome the limitations of conventional security and system management technologies. These capabilities come from both the innate properties of the BigFix Core Services Platform and specific tools and capabilities that can be managed through the BigFix Console.

At the platform level, the BigFix single agent/single management infrastructure brings consolidated real-time visibility and control to enterprise-wide security and configuration management. The BigFix Agent provides real-time information on the configuration and state of every device it runs on—mobile or fixed—with no scanning required. The BigFix Agent also runs on Windows, Linux, Unix and Mac OS systems, with these devices visible and manageable through the BigFix console.

Perhaps the most important property that BigFix brings to NAC is the ability to manage both fixed and mobile computers at equivalent levels of visibility and control. Managing mobile laptop/notebook computers is a long-standing BigFix strong suit. The BigFix Agent remains resident on mobile computers whether they are connected to the enterprise network or not. Policies remain in force on mobile systems until changed by enterprise IT managers. Roaming computers can also be instructed to make contact with the enterprise network to transmit configuration change information and receive policy and management content (software updates, new policies, patches, etc.) any time the mobile device connects to the Internet.

BigFix complements the capabilities of the BigFix Core Services Platform with a growing array of tools and capabilities that enable automated discovery, assessment, remediation, and enforcement of security policies. Current capabilities include asset discovery and inventory, antivirus, anti-spyware, personal firewall, vulnerability assessment and remediation, operating system and application software update and patch management, and technical controls compliance reporting.

### **Enabling Effective NAC through BigFix**

Adding BigFix to a NAC solution should sharply reduce the number of devices caught in quarantine through BigFix's pre-mediation capabilities. For those caught in quarantine, BigFix can automate and speed the process of identifying device configuration deficiencies and correcting them.

Of course, not every machine attempting to access a network—particularly those used non-employee business partners—will have BigFix installed on it. Here, assuming the machine's owner consents to this as a condition of doing business, it is possible to temporarily install a BigFix Agent on a guest computer, assess its configuration, remediate it, and uninstall the Agent when the machine exits the enterprise network.

BigFix also opens the door to another intriguing possibility—implementing a BigFix solution that performs NAC-equivalent functionality without need to invest in additional dedicated NAC hardware and software. Since BigFix can continuously monitor and adjust device configurations in real-time, detect and isolate rogue and non-compliant devices, and generally provide functionality comparable to dedicated NAC solutions with less expense and management complexity, implementing a BigFix-based virtual NAC merits consideration by those who want to add a preemptive block-the-bearers-of-threats capability to their IT security program.

NAC can only be effective when coupled with a program of continuous policy enforcement of managed systems. Quarantining devices should be a last resort and not the main method to secure an environment. Until recently, most security and configuration management solutions could not provide the comprehensive, continuous visibility and control required to enable managed devices to avoid unnecessary visits to quarantine limbo. BigFix, however, offers capabilities that can significantly enhance the effectiveness of NAC solutions. While after an initial burst of industry enthusiasm, NAC has lost momentum as the next big thing in enterprise information security, BigFix offers technologies and solutions that can revive the viability of NAC solutions by improving their flexibility and cost effectiveness.

### **BigFix Asset and License Management**

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.

### **Infrastructure Picture Window**

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 note book 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.

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.

Finally, 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 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 opens 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 many 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.

### **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.

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.

### **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.

**Summing Up:**

Historically, IT security and system management has been far too reactive. Security staffs see their jobs as responding to incidents and emergencies. New products come on to the market after a new threat captures headlines, but add complexity even as they solve the problem of the day. Ineffective tools with poor first-pass-success rates bog IT staffs down with remedial busy work, diverting them from higher return activities. BigFix, by aligning IT processes with change rather than resisting it, challenges the IT status quo at many levels.