

WHITE PAPER



THE POWER OF ONE - GLOBAL IT VISIBILITY AND CONTROL AT THE VELOCITY OF BUSINESS CHANGE

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

Business runs at a velocity unimagined a few short years ago. Complex and highly distributed environments have grown to support an intricate web of partners, suppliers, distributors, and customers. Service oriented architectures and web-based applications have progressed from vision to real-world instantiation as enterprises look to leverage technology to innovate and deliver new services. In this new world, IT-delivered services must be available 24x7 to customers, suppliers, employees, regulators, investors and other constituencies.

The highly exposed nature of today's IT infrastructures fundamentally changes how organizations manage IT assets, processes and data. IT organizations can no longer treat resource management and maintenance as back-end functions that can be performed at times and conditions of their choosing. Neither is their work protected from outside scrutiny. Processes whose success or failures were largely internal now make the difference between business success or failure, legal compliance or litigation, prudent stewardship or ineffective execution.

To meet these requirements, IT organizations urgently need to migrate to a new kind of security and system management platform. The new model platform will combine radical improvements in ability to see and control IT assets and data in real-time while consolidating and reducing infrastructure management costs. In transforming IT infrastructure management, the new platform will change the long-standing imperative of “doing more with less” from a recipe for compromise to a gateway to new levels of management and value generation.

Four Mandates for IT Organizations

IT has four major responsibilities in helping enterprises succeed. First, they must deliver continually improving service quality and market-leading agility to their business. Second, they must align with other business functions in improving control and utilization. Third, they must address security risks to information, business continuity, brand integrity, and IT assets. Fourth, they must demonstrably control IT processes, information, and infrastructure to the satisfaction of governments, regulators, and the public.

In meeting these responsibilities, IT managers can no longer incrementally buy new tools to meet any new requirement that makes headlines in the technical or business media. Business value, security and compliance mandates converging on the enterprise require a converged response. CIOs demand solutions that enable them to eliminate redundant technologies and processes and integrate disparate elements into a common workflow. While established enterprise software vendors have adopted the language of convergence and consolidation, their product lines remain tied to the past for business and technical reasons. Proposing radical change to their customers carries the risk of disrupting established revenue flows not to mention technical risks inherent in overhauling or replacing obsolete products.

As established vendors hang on to trailing-edge technologies, IT organizations should begin their search now for the next generation of infrastructure management platform. At this point it is important to distinguish platforms from tool sets.

Platforms provide baselines and channels for formulation, delivery, reporting and evaluation of infrastructure management services. In many ways, their most important function lies in creating a consolidated, long-term metaphor for management service delivery. Tools and services delivered by the platform may come and go over its lifetime, but a stable, durable platform enables IT staffs to focus their efforts and develop deep expertise in service delivery processes. Tool sets may include a number of immediate remedies, but carry with them individuated interfaces, methodologies and ways of doing things. These often clutter the minds of IT staffs with tool-specific trivia every bit as much as their deliverables of appliances, software and manuals do to management infrastructure itself.

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.

Four IT Imperatives

- **Service Delivery**—Requiring improved quality and agility in service quality to the business.
- **Cost Reduction and Efficiency**—Requiring improved control and better utilization of assets and labor.
- **Risk Management**—Addressing security risk to information, business continuity, and IT assets.
- **Regulatory Compliance**—Requiring demonstrable control of IT processes, information, and infrastructure.

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: The Power of One

One Platform

- Unified IT Security and IT Infrastructure Management process optimization
- Massively scalable and lightweight distributed processing architecture
- Highly extensible and customizable
- Segmentation of stable core services platform and rapid deployment problem-space focused policy libraries

One Agent

- Distributed client (self) management model
- Multifunction--the agent as a universal policy execution machine
- Low-impact-minimal demand for client processing or network communications bandwidth
- Heterogeneous operation-Agent ported to widely-used operating systems (Windows, Unix, Linux, Mac OS), with all clients manageable through a common management control console

One Solution

- Real-time automated policy-driven process execution
- Ad-hoc problem detection, remediation, and reporting
- Highly secure
- Consolidate and manage third-party applications through a common visibility, communications and control infrastructure

Significant ROI Advantages Over Alternative Approaches

- Rapid deployment
- Easy to use and manage
- Staff labor savings
- Fast, complete remediation cycles
- Higher first-pass-success rates
- No exceptions" management of fixed, mobile, local and

ment 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.

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 Solution Packs

As discussed above, BigFix provides a powerful and flexible platform for delivery of security and system management services to networked enterprise infrastructures. With this core services platform in place, it becomes possible for BigFix to develop and license a growing portfolio of specific services deliverable over the BigFix Core Services platform.

BigFix Solution Packs group together collections of policy content modules focusing on high priority enterprise IT problem spaces. The current line of BigFix Solution Packs features BigFix AntiThreat, an integrated approach to security threat suppression; BigFix

WHITE PAPER

IT Policy Enforcement, addressing process and human risks to enterprise integrity; and BigFix Desktop and Server Management automating and simplifying common system management tasks. By relying on the BigFix Core Services Platform as their delivery vehicle, all BigFix solution packs bring a common, consolidated management methodology to their functional areas. This not only consolidates and standardizes delivery of previously separate services, it helps deepen staff expertise in this management methodology, improving productivity and reducing error risks.

BigFix AntiThreat Solution Pack

The BigFix AntiThreat Solution Pack brings together the three most important anti-malware defense services-antivirus, anti-spyware, and personal firewall-and makes them seamlessly manageable through the BigFix Console and the BigFix Agent. The product

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. The Solution Pack sets the stage for proactive, preemptive, policy-driven anti-malware threat suppression at enterprise scale.

Real-World Results

- Major mortgage lender reduced the number of FTE administrators dedicated to server patching by a ratio of four to one.
- One \$6,000-class server manages 180,000 endpoints at a major health maintenance organization.
- Communications company saves \$1.5 million in software licensing costs after using BigFix to analyze usage patterns.
- Pharmaceutical company reports that moving from 70% first pass success for server patching to 98% saves the company \$700,000 in IT service costs annually.
- West coast healthcare provider saves \$2.5 million by using BigFix to audit software licenses in use against prevailing contracts.
- BigFix users locate laptop computer batteries subject to manufacturer recall within minutes after launching custom Fixlet message.

BigFix IT Policy Enforcement Solution Pack

The BigFix IT Policy Enforcement Solution Pack consolidate key security configuration management services including network access control, patch management, application execution controls (white and black lists), vulnerability management, and automated security configuration management to cut costs, reduce complexity, lower security risks and move information security programs from reactive fire-fighting to proactive, preemptive risk management.

BigFix Desktop and Server Management Solution Pack

The BigFix Desktop and Server Management Solution Pack brings BigFix operational excellence and economics to key IT operational tasks including asset discovery/inventory, software license tracking, power management, software distribution, patch management and configuration management. This Solution Pack automates many of the mundane IT management and maintenance tasks, eliminating manual drudgery as well as “push and pray” uncertainty, freeing IT staffs to focus on high value initiatives. Best of all, IT staff drive desktop and server management tasks through the same BigFix infrastructure and management console they use for external threat suppression (BigFix AntiThreat™) and security policy enforcement (BigFix IT Policy Enforcement) Solution Packs.

Summing Up: The Power of One

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.