BIGFIX

Continuous Situational Awareness with BigFix

Executive Summary

Situational awareness is the ability to quickly understand environmental variables. The actionable intelligence can drive faster response times, better informed decisions, and higher IT service levels.

BigFix provides the pervasive real-time asset visibility that enables an organization to obtain situational awareness into all computing assets, their current state, and all dynamic changes they may be experiencing. By offering complete, accurate and up-to-the-minute situational awareness, BigFix serves as the single source of truth into the state of all organizational computing assets located anywhere—fixed or mobile, physical or virtual.

"BigFix has truly lived up to its name. When the time came to install it was working within a couple hours. We consolidated our server and workstation management, patch management, policy compliance, and vulnerability assessment tools all into BigFix, which allowed us to cut the upfront cost, as well as ongoing maintenance costs in more than half. We are still early in operation, but from what I've seen so far BigFix is hands-down the best tool for server and workstation management that I've used to date."

–Senior IT Engineer
Large Defense Contractor

Observe, Orient, Decide and Act

For the most part, systems and security management has been a reactive process—for example, once an incident occurs, how quickly can we resolve the condition? But as organizations become more reliant on technology, and, as we move to achieve higher service levels and improved customer experience, IT must implement controls that will limit the probability of an incident from occurring in the first place.

There is no fail-safe in today's digital world—incidents will occur, both unintentional and malicious. However, when they do, the agile organizations will respond quickly to mitigate damage and organizational impact. The challenge is that this level of agility requires pervasive real-time visibility and control over all computing assets to not only identify deviations from accepted operating state but to quickly return the environment to homeostasis.

USAF Colonel and military strategist John Boyd created the concept of the OODA loop[1] to define combat operations. It is applicable to both military and commercial operations and is well-suited for mission-critical computing in a highly dynamic threat environment:

- **Observe** through situational awareness all aspects of the computing environment.
- **Orient** the information to the specific environmental conditions in real-time.
- **Decide** the best course based on actionable intelligence.
- **Act** to quickly respond and resolve incidents that impact the organization.

Much like Col Boyd's cyclical OODA process, to become more effective and efficient requires continuous assessment of the state of one's environment and the complex interactions between systems, applications, and the infrastructure that supports them. With sophisticated and automated technologies combined with trained personnel, organizations can become more mature and agile.

How BigFix Enables Organizations to Obtain Situational Awareness

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 organizations can reduce management complexity and immediately improve productivity, service, and coverage. This approach enables organizations to significantly reduce costs in the short term and over time.

Pervasive asset discovery and control

Corresponding to the "observe" component of the OODA model, BigFix offers unparalleled discovery of assets on both a macro and a micro level, ensuring that software records are up-to-date, accurate, and complete. At the macro

[1] http://en.wikipedia.org/wiki/OODA_Loop

BigFix offers unmatched inspection and remediation, with the ability to see and control thousands of inspectable and reportable computer properties out of the box.

level, BigFix can discover any BigFix-managed asset regardless of connection state—on or off the network, virtual or physical—and across a number of operating systems and topologies in a heterogeneous environment.

BigFix also offers auto-discovery of assets on the network that are not managed by BigFix including those that may be unauthorized or pose a threat. BigFix can automatically deploy agents to those assets which should have access to the network, as well as enforce configuration policy checks prior to allowing access.

At the micro level, BigFix customers enjoy up-to-the-minute visibility into the most granular properties and processes across tens of thousands, or even hundreds of thousands, of computing assets. BigFix offers unmatched inspection and remediation, with the ability to see and control thousands of inspectable and reportable computer properties out of the box. BigFix enables administrators to define baseline configurations for device types based on any of these device properties. And with BigFix, IT can discover the applications installed in a company's infrastructure down to the version level.

Continuous asset visibility

BigFix can provide a real-time view into problems that exist in the environment, rather than wait for returns on weeks-old inventory scans. The BigFix Console provides a single operational view into the agency infrastructure for comprehensive visibility and control across distributed global networks. IT operators can instantly see the configuration settings that need to be evaluated and the assets that are not compliant. Operators can schedule control and remedial actions in change control windows within minutes, and receive immediate validation that the action has completed successfully.

This real-time visibility and control reduces the load on the network infrastructure, the server, and the assets themselves while shortening and reducing ambiguity of query/remediation actions. It also allows IT organizations to implement critical management functions for hundreds of thousands of endpoints from a single unified management console. BigFix customers enjoy real-time visibility into security-critical endpoint configurations, helping to avoid security breaches, lost productivity, and compliance issues while preventing overspending. Multi-platform support across Unix, Linux, Mac and Windows means broad coverage, as well as deep visibility.

Securing computing devices against configuration errors

Many organizations are mandated to protect their computing assets by implementing technical safeguards such as hardened configuration settings on information systems, ensuring that systems are patched appropriately, and conducting risk management against known vulnerabilities to determine organizational exposure. BigFix helps by providing continuous, accurate, and comprehensive visibility and control into the security posture of every endpoint on the infrastructure.

BigFix offers persistent discovery and visibility, ensuring that software is up-to-date, accurate, and complete.

By bridging configuration assessment with automated remediation, BigFix enables organizations to:

- Enforce policy compliance so that systems do not drift from required security configurations, such as FDCC or DISA STIGs
- Validate that systems are patched and updated appropriately and within reasonable timeframes
- Reduce overall exposure to risk due to vulnerabilities and exploits that take advantage of known misconfigurations or unpatched systems
- Monitor external devices and removable media (iPods, USB thumb drives, etc.), which are often the source of data leaks.

Protecting data from attacks

Organizations must further mitigate risk by ensuring that systems are kept up-to-date with their endpoint protection solutions and automatically remediate vulnerabilities through continuous policy enforcement. Whether the organization uses BigFix anti-virus products or third-party anti-virus suites, BigFix can provide:

- Comprehensive monitoring of all endpoint protection products from a single console
- The ability to identify systems running old DAT files or whose anti-virus services are turned off or configured improperly

BigFix Addresses the Broader Challenges of Effective Systems and Security Management

Beyond the specific requirements of federally mandated compliance initiatives, IT organizations face a number of challenges in achieving effective, efficient systems management:

- Slow speed of management tasks across a highly distributed enterprise network
- Poor visibility into and lack of validation from distributed assets
- Difficulty managing multiple, heterogeneous infrastructures
- Limited IT staff resources
- Mission-critical systems that require “always up” availability

For each challenge area, BigFix offers features that meet the needs of IT organizations:

- Superior speed through real-time endpoint processing
- Comprehensive visibility
- Multiplatform support
- Centralized management with ease of use
- Rapid implementation and automated remediation

With BigFix's unified management model, customers can simplify and automate infrastructure management, saving costs and improving service delivery.

Challenge: Poor visibility and long lag times, translating to poor currency of data and increased risk. For most tools, updated visibility into endpoint status occurs only during an inventory cycle—which may take place as infrequently as once a week. As a result, IT doesn't know the state of computing devices. After software delivery, this poor visibility prevents IT from getting accurate validation that software has been delivered and installed correctly—either across all endpoints or for a single endpoint. This also exposes the organization to increased risk and overspending on software that may be unauthorized or unnecessary.

With BigFix: Comprehensive, pervasive, accurate, historical visibility for all assets—managed or unmanaged. BigFix offers persistent discovery and visibility, ensuring that software is up-to-date, accurate, and complete. The solution can provide visibility into any asset regardless of its connection state. The BigFix console provides a single operational view into the infrastructure for comprehensive visibility and control. Operators can instantly see the configuration settings that need to be evaluated and the assets that are not compliant.

Challenge: Complex, resource-intensive management of multiple, heterogeneous infrastructures. Many IT infrastructures include a multitude of legacy systems and must manage assets running on a variety of platforms.

With BigFix: Multiplatform support. BigFix's multiplatform support simplifies administration of heterogeneous environments—including those with legacy systems and applications. The BigFix suite has the ability to service environments running multiple generations of Windows as well as Unix, Linux, Mac, mobile, and virtualized computers through integration with the management infrastructure.

Challenge: Maintaining high-quality IT service levels with limited staff and budget. Many IT organizations must find creative ways to manage an ever-expanding asset pool with small (and often shrinking) human and financial resources.

With BigFix: Single-console architecture offering streamlined, simplified management. The BigFix solution is delivered and managed by the BigFix Unified Management Platform for a single-console, single-management server experience across systems lifecycle management, endpoint protection, and security and configuration management. With BigFix's unified management model, customers can simplify and automate infrastructure management, saving costs and improving service delivery. Many unnecessary operational tasks can be eliminated and others significantly streamlined, resulting in abbreviated cycle times. Additionally, IT staff does not need to learn how to operate multiple management frameworks.

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.

Challenge: Mission-critical systems that require "always up" availability. Whatever the scope of your organization's service offerings, even a short period of downtime can negatively impact both internal and external stakeholders—from minor inconveniences to major downtime. With so much service delivery based online, the IT organization becomes the center of mission-critical operations.

With BigFix: Rapid time to value and automated remediation. BigFix offers IT the ability to automatically remediate security and health issues on computers wherever they reside in the network. As soon as a misconfiguration or unpatched asset is detected, operators can schedule remedial actions in change control windows within minutes, and receive immediate validation that the action has completed successfully. This helps eliminate system or security breaches that could compromise data residing on an endpoint.

Challenge: Slow implementation and response times for IT management tasks across the distributed enterprise. While many networks stretch across a region, a country, or the globe, network infrastructures struggle to keep up. Many enterprise infrastructures run over low-bandwidth, high-latency networks. As a result, system and security management tasks can take up a high percentage of available bandwidth, slowing network performance—and end user productivity.

With BigFix: Blazing speed thanks to intelligent agent processing. In distributed environments with roaming endpoints, true speed, accuracy, and efficiency requires a model where processing is conducted on the endpoint itself. With BigFix, having the assessment and analysis conducted on the endpoint increases the speed of asset discovery, software delivery, and validation. Less communication is required between the server and endpoint, increasing speed and reducing the amount of network bandwidth consumed. Without waiting for a centralized server to finish performing a compiled analysis of asset data, the IT operator is able to receive answers to inquiries on assets within minutes.

A Closer Look at BigFix Support for IT Organizations

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 organizations can reduce management complexity and improve productivity, service, and coverage. All this, plus reduced costs.

The key solution components in the BigFix offering are:

- BigFix Asset Discovery delivers pervasive visibility and control to IT operations—ensuring that organizations identify all IP-addressable devices quickly, with minimal network impact.

- BigFix Security Configuration and Vulnerability Management consolidates services including security patch management status, vulnerability management, and automated security configuration management to cut costs, reduce complexity, and lower security risks.
- BigFix Client Manager for Endpoint Protection enables management of third-party endpoint security clients and brings unprecedented scalability, speed, and thoroughness to keeping organizations ahead of external threats.
- BigFix Endpoint Protection consolidates disparate systems and security management tools into a single console, single infrastructure solution that can improve reaction times to security incidents and decrease the impact of managing multiple infrastructures.

The BigFix Unified Management Platform is the backbone of the overall BigFix solution which is comprised of 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/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 efficiency, while maintaining a high level of commitment to service delivery.

BigFix: Breakthrough Technology, Revolutionary Economics

Founded in 1997, BigFix®, Inc. 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. Today, BigFix provides real-time visibility and control for over 8 million computing devices for 900 customers worldwide. 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.