BIGFIX

BigFix: Enabling SANS 20 Critical Controls / NIST 800-53 For Compliance

Executive Summary

Cybersecurity is becoming one of the nation's highest priorities. To address growing concerns, the National Institute of Standards and Technology (NIST) has issued security guidelines, in NIST Special Publication 800-53 revision 3, which provide a comprehensive set of security controls designed to facilitate securing our nation against cyber attacks. In an effort to narrow the focus of the guidelines to a fiscally manageable state without compromising the requirements, current and past federal CIOs and CISOs established a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms. They were able to identify 20 specific technical security controls that effectively block known high-priority attacks, as well as those attack types expected in the near future and that can be applied across agency enterprise environments and potentially across the Federal government.

At BigFix we know that every Federal security program is founded upon accurate and real-time visibility into system and security configuration for all endpoints, including those that are mobile and roaming, as well as across platforms. Further, gaining unified visibility and control over "virtualization sprawl" simplifies IT operations, reducing risk and systems management costs. Typically a comprehensive approach requires a combination of complementary technologies.

BigFix provides the pervasive real-time asset visibility and continuous monitoring that enables an organization to obtain situational awareness into all computing assets, their current state, and all dynamic changes they may be experiencing. BigFix systems and security management enables a multi-layered, defense-in-depth strategy. Additionally, the BigFix Unified Management Platform can be rapidly deployed and leverages your existing infrastructure. 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.

Continuous Coverage on Eight of the 20 Critical Controls with BigFix

Today's Federal IT operations and security teams are tasked with monitoring, detecting, analyzing, protecting, reporting, and responding against known vulnerabilities, attacks, and exploitations. The only way to meet this challenge is to continuously test and evaluate information security controls and techniques to ensure that they are operating effectively. BigFix offers IT operations and security teams a successful systems and security management for 8 of the 20 critical controls with an approach that relies on accurate, real-time and pervasive visibility into the existing environment. BigFix's single agent, distributed intelligence infrastructure provides a cost-effective approach for continuous compliance. By relying on BigFix as one of the critical foundational technologies for managing mandated security programs, teams can meet internal and external guidelines while dramatically reducing costs.

Critical controls covered by BigFix are:

CC1: Inventory of Authorized and Unauthorized Devices

CC2: Inventory of Authorized and Unauthorized Software

CC3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

CC8: Controlled Use of Administrative Privileges

CC10: Continuous Vulnerability Assessment and Remediation

CC12: Malware Defenses

CC13: Limitation and Control of Network Ports, Protocols, and Services

CC14: Wireless Device Control

For each control area, BigFix offers features that support all cybersecurity efforts:

- Comprehensive visibility
- Detailed, real time inventory
- Continuous monitoring
- Enforce policy compliance
- Continuous coverage
- Single console, single infrastructure malware solution
- Endpoint security
- Scalable, flexible asset discovery

Challenge: CC1: Inventory of Authorized and Unauthorized Devices

Associated NIST SP 800-53 Controls for FISMA Compliance: CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6

The most common way to compromise a network is through unknown and/or unprotected systems, out-of-date devices, and new hardware installed but not immediately configured and patched. Moreover, attackers who have already gained internal network access frequently seek out and jeopardize additional improperly secured internal computer systems for future access. Test systems briefly connected to the network and, subsequently, not usually included in the standard asset inventory of an organization, provide another avenue in. To effectively manage the asset security, organizations need a strong security infrastructure where all devices and changes to devices, on and off the network, are identified and tracked.

BigFix Solution: Comprehensive visibility. The BigFix Asset Discovery & Inventory module provides comprehensive visibility into any IP-enabled device found on and off the network, including network routers, switches, firewalls, IDS sensors, printers, etc. BigFix initially scans the network for new devices and reports back if they are being managed by BigFix. The report also includes information about the device—device type, OS, hostname, IP address, Mac address, etc., and each successive scan reports on only new devices found. BigFix scanning technology uses the BigFix distributed relay infrastructure to minimize impact and increase frequency, providing near real-time updates. And scans can be scheduled at any interval. Once the BigFix agent is installed, it will use the full set of inspectors to report back on thousands of properties and additionally report back if any of these properties change without the need to schedule scans. BigFix's distributed scanning technology typically uncovers 15%-30% more assets on the network than previously identified. By taking advantage of the pervasive visibility and control provided by BigFix Asset Discovery, IT operations can quickly and easily identify all IP-addressable devices quickly, with minimal network impact.

CC2: Inventory of Authorized and Unauthorized Software.

Associated NIST SP 800-53 Controls for FISMA Compliance: CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9, PM-6, SA-6, SA-7

Typically, most systems exploitation occurs through software vulnerabilities. Organizations are often unable to find vulnerable or malicious software to mitigate problems or root out attackers because they are lacking complete software inventories. Further, installing software—either a patch or an entirely new application—can potentially create another entry point for attackers. The only way to secure your systems is by inventorying and controlling what programs are installed and running.

BigFix Solution: Detailed, real time inventory. BigFix provides deep and continuous visibility into the configurations and applications installed and used on corporate IT assets on and off the corporate network. This capability provides the detailed, real time inventory about installed executable code, versions, and patch levels required to ensure the assets are not compromised and remain secure. The core of this capability is the BigFix agent, which continuously reports, in real time, installed executables, application usage data, and other forensic data about software, including easily customizable information such as a cryptographic hash. This information is normalized and accessed through solutions like the BigFix DSS Software Asset Management module for flexible asset management reporting—e.g., determining what's installed where, usage patterns, and even license compliance information—and also leveraged in partner-integrated solutions like the Bit9 Parity solution for application whitelisting and malicious software launch prevention. By leveraging BigFix, not only can IT Operations discover vulnerabilities, but they can also remediate those vulnerabilities quickly, and then continuously enforce remediation.

CC3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers.

Associated NIST SP 800-53 Controls for FISMA Compliance: CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6

Standard configurations are often geared to ease-of-deployment and ease-of-use and not security, making it easy for attackers attempt to exploit both network-accessible services and browsing client software using such techniques. To ensure security, most systems require a hardened image customized for the organization using the device. And to guarantee that these images have a sound level of security, you need proper configuration management with tested and validated images that are maintained through a strict change control process that includes updates, to the secure image, to overcome ever evolving threats to your network.

BigFix Solution: Continuous monitoring. The BigFix Security Configuration and Vulnerability Management module provides organizations with continuous monitoring of security configurations, patches, and vulnerabilities of UNIX, Linux, and Windows based systems. BigFix supports the configuration standards defined by DISA, NIST, and others and is fully validated as an FDCC scanner, authenticated configuration scanner, authenticated vulnerability and patch scanner, and misconfiguration remediation. The BigFix agent provides complete real-time monitoring and assessment of configuration policy and reports on any policy deviations identified. BigFix can enforce configuration policy on the endpoints and provides closed-loop confirmation of success or failure. Using BigFix Security Configuration and Vulnerability Management, IT operations can consolidate services including security patch management status, vulnerability management, and automated security configuration management to cut costs, reduce complexity, and lower security risks.

CC8: Controlled Use of Administrative Privileges.

Associated NIST SP 800-53 Controls for FISMA Compliance: AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)

Every device operating system requires some kind of system account that is all-powerful—i.e., granting the ability to control everything on that system. Microsoft Windows operating systems call this an "administrator" account. In the UNIX, Linux, and Mac world, it is known as the "root" account. To make sure attackers have a little chance possible to gain administrative privileges, you must ensure that these privileges are used as little as possible. The ideal way to do this is to configure all user accounts with non-administrative permissions. Using NIST configured and tested security templates is the most efficient easiest way to conform to configurations stated in the NIST 800 series publications. Applying these templates, however, can be time-consuming.

BigFix Solution: Enforce policy compliance. BigFix provides the ability to centrally manage, monitor, and enforce policy related to administrative and non-administrative system access at the local policy level. Organizations that desire to define policies for password enforcement, including length, complexity, retention, re-use, and lockout policy can configure the policies within the BigFix Management Console and enforce policies on any managed endpoint. The revolutionary BigFix architecture is powered by a distributed intelligent agent infrastructure that continuously monitors and manages policy compliance regardless of network connectivity, across a variety of platforms, without impacting endpoint performance. Building on a cost-effective, unified management platform, BigFix automates enterprise-scale policy enforcement, power conservation without compromising network performance, end-user productivity, or security. In many environments, installing BigFix has significantly reduced system administrator workloads while improving the effectiveness of system management.

CC10: Continuous Vulnerability Assessment and Remediation.

Associated NIST SP 800-53 Controls for FISMA Compliance: RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)

While vendors are searching for remediation, attackers are engineering exploit code and launching it against targets of interest making discovering and reporting vulnerabilities a double-edged sword. What this means is you must continuously scan for any vulnerabilities and immediately address discovered flaws to reduce the likelihood of systems compromise.

BigFix Solution: Continuous coverage. The BigFix platform is designed to continuously discover, assess, remediate, and enforce the health and security of servers, desktops, and roaming laptops in real-time via a single, policy-driven agent and single console. The BigFix Agent provides visibility and control over policies related to vulnerabilities, patches, and configurations and enables enterprises to identify and resolve problems at scale, in real-time. As policy deviations are identified, they can be resolved by implementing patches, installing software updates, or remediating mis-configured systems. Results are available via the reporting engine, enabling users to generate closed-loop confirmation of success, changes over time, and delay measurements as compared to organizational SLAs. BigFix provides granular system targeting to support change control—i.e., test environment /production environment. Also included is a completely automated path for continuous vulnerability assessment and remediation. By leveraging BigFix Security Configuration and Vulnerability Management, IT Operations can consolidate services including security patch management status, vulnerability management, and automated security configuration management to cut costs, reduce complexity, and lower security risks.

CC12: Malware Defenses.

Associated NIST SP 800-53 Controls for FISMA Compliance: SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)

Malicious software—Malware—targets end-users and organizations via web browsing, email attachments, mobile devices, and other vectors. Its sole purpose is to attack and take advantage of systems and other software by tampering with the system's contents, capturing sensitive data, and spreading to other systems. Anti-malware tools, also referred to as anti-virus and anti-spyware software, is designed to help defend against malicious threats by attempting to detect malware and block its execution. Modern malware comes in many forms and some is capable of disabling anti-virus tools running on the targeted system. Therefore, the most effective protection methods should be in the form of stacked or layered defenses.

BigFix Solution: Single console, single infrastructure malware solution. The BigFix Endpoint Protection suite brings together world-class anti-malware from Trend Micro, with multi-vendor management, endpoint firewall management, and network access control under a single infrastructure. Consolidating management of heterogeneous clients through a common visibility and control infrastructure improves IT staff effectiveness. For example, BigFix can tell you not only which endpoints might have fallen behind in their anti-virus definition updates, but correlate this with endpoints that may be running non-standard and rogue applications. In addition, BigFix provides the Client Manager for Endpoint Protection to facilitate the management of third-party endpoint security clients from vendors such as CA, IBM, McAfee, and Symantec. This allows for BigFix to watchdog these malware products and ensure that signature files are updated appropriately, services are started, and the tools remain generally healthy. BigFix also provides configuration control over USB and other communication devices—Bluetooth, IR, etc.—and includes a network access control integration with known NAC vendors to provide comprehensive command, control, and remediation capability for allowing system access to the network. BigFix's Client Manager for Endpoint Protection brings unprecedented scalability, speed, and thoroughness to keeping organizations ahead of external threats. By consolidating disparate systems and security management tools into a single console, single infrastructure solution, BigFix Endpoint Protection improves reaction times to security incidents and decreases the impact of managing multiple infrastructures.

CC13: Limitation and Control of Network Ports, Protocols, and Services.

Associated NIST SP 800-53 Controls for FISMA Compliance: CM-6 (a, b, d, 2, 3), CM-7 (1), SC-7 (4, 5, 11, 12)

Poorly configured web servers, mail servers, file and print services, and DNS servers installed by default on a variety of different device types, often without a business need, are network services most vulnerable to attack. Further, software packages oftentimes automatically install services and turn them on, without informing a user or administrator that the services have been enabled, as part of the installation of the main software package. These services are ripe for attack, and attackers always scan issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code. To maintain security, it is imperative that you seal all and secure or monitor those that must be open.

BigFix Solution: Endpoint security. BigFix is the only endpoint security and system management solution that provides pervasive real-time visibility and control in large, complex, distributed environments, especially those with bandwidth concerns and limited IT staff. The BigFix Endpoint Protection suite includes an endpoint firewall product and NAC solution that secures endpoints on the network off the network by protecting them with an integrated endpoint firewall and network access control strategy. The host-based firewall can be configured with default rules that drop all traffic other than what is explicitly allowed. As an alternative, customers can use the BigFix Security Configuration Management product to leverage the FDCC firewall rules for the Windows firewall. Either BigFix solution is uniquely designed to meet the exacting Federal requirements while at the same time reducing overall IT costs and improving endpoint security. BigFix also extends the reach of centralized visibility and control throughout networks, dramatically improving system security and vulnerability protection. And all of it is done with a minimum of additional, dedicated equipment.

CC14: Wireless Device Control.

Associated NIST SP 800-53 Controls for FISMA Compliance: AC-17, AC-18 (1, 2, 3, 4), SC-9 (1), SC-24, SI-4 (14, 15)

Wireless technology introduces a mobile threat that complicates security operations because it is difficult to control. Attackers have used proximity to bypass security parameters and connect wirelessly to vulnerable access points. Further, wireless clients used by personal working remotely are prime targets for attackers who exploit systems and use them as back doors when they are reconnected to the network of a target organization. In sum, the lack of a direct physical connection makes all wireless devices convenient vector for attackers to maintain long-term access into a target environment. To maintain corporate security and reduce operational risk, all wireless assets must be identified and assessed.

BigFix Solution: Scalable and flexible asset discovery. The BigFix Asset Discovery module allows enterprises to proactively reduce risk and continuously enforce policies by identifying suspicious or rogue systems entering the network. BigFix can automatically deploy agents to those assets that should have access to the network, as well as enforce configuration policy checks prior to allowing access. By using asset auto-discovery, IT Operations can identify and locate assets on the network that are not managed by BigFix including those that may be unauthorized or pose a threat. Through the flexibility of the BigFix managed agent, any agent can be designated as an asset discovery scan point. Once a scan point is designated, the discovery process identifies any IP device connected to the network, including wireless access points. A wizard is provided for configuring and scheduling schedule scans. Scan point uploads include only the differences from the last scan. BigFix can also scale to even the largest of environments quickly and painlessly—a single server supports up to 250,000 endpoints distributed across the globe with all types of connections. With BigFix Asset Discovery, IT operations have pervasive visibility and control for ensuring that all IP-addressable devices are identified quickly, with minimal network impact.

Extending the BigFix Platform

BigFix offers companies real-time visibility to enhance existing third-party technologies. Thanks to the open architecture of BigFix's Unified Management Platform, organizations can leverage its real-time visibility to "feed" rich content to external systems like CMDB's and SIEM tools. Our experienced Professional Services organization provides onsite assistance to customize the integration from the planning stages throughout an implementation program enterprise-wide.

The BigFix Federal Solutions Suite

BigFix has a proven track record in providing security and IT operation solutions to government. Whether it's for a federal civilian agency, the Department of Defense, the Intelligence Community or state and local governments, BigFix has a proven real-time situational awareness and remediation platform for all IT assets regardless of OS, location or network connectivity status. Best of all, BigFix is compliant under the following certifications and available for procurement as follows:

- Common Criteria Certified (EAL Level 3)
- FIPS 140-2 Level 2 Certified
- ESI and SmartBUY BPA Award
- GSA Schedule 70
- Security Content Automation Protocol (SCAP) Certified

Government customers have purchased BigFix to help manage over 600K endpoints across Civilian and DOD. They have done so to address a variety of challenges, government mandates (e.g., SCAP FDCC), projects (e.g., DAR encryption, NAC) and initiatives (ITIL) that includes: improving asset visibility, reducing and eliminating costs via power reduction and management efficiencies, providing accurate and timely patch management and patch validation, achieving configuration/compliance for FDCC/DISA STIGS/other, management of software assets, improving endpoint security posture and more. BigFix has combined key components of our existing solution packs and combined them into a specific, Federally focused suite to address all of the above.

The key solution components in the BigFix Federal Solutions Suite for addressing the 20 Critical Controls are:

- **BigFix Asset Discovery & Inventory** (CC1, CC2) delivers pervasive visibility and control to IT operations—ensuring that organizations identify all IP-addressable devices quickly, with minimal network impact.
- **BigFix Software Asset Management** (CC2, CC14) (optional add-on component) reduces software licensing costs through correlation of real-time software usage with contract licensing information.
- **BigFix Security Configuration and Vulnerability Management** (CC3, CC8, CC10) consolidates services including security patch management status, vulnerability management, and automated security configuration management to cut costs, reduce complexity, and lower security risks.
- **BigFix Patch Management and Software Distribution** (CC2, CC10) provides distribution and implementation of security patches, offering a 95%+ first-pass success rates and multi-platform support.
- **BigFix Client Manager for Endpoint Protection** (CC12) 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** (CC13) (optional add-on) 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.

In addition to these modules, the BigFix Federal Solutions Suite includes Power Management for near-immediate payback on your purchase. Customers have seen savings of $15-$50 per endpoint per year while enjoying sophisticated controls that ensure power settings do not interfere with security, maintenance, and end-user productivity needs.

A Closer Look at the BigFix Unified Management Platform

BigFix offers centralized administration, complete automation, real-time visibility into remediation processes, and the “exibility” to solve cybersecurity challenges that IT organizations face both now and in the future. By using one BigFix toolset and one unified infrastructure, IT organizations can comply with guidelines, secure internal and external systems, without impacting productivity, service, coverage, and cost.

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. This information is normalized and accessed through solutions like the BigFix DSS Software Asset Management module for flexible asset management reporting—e.g., determining what's installed where, usage patterns, and even license compliance information—and also leveraged in partner-integrated solutions like the Bit9 Parity solution for application whitelisting and malicious software launch prevention.

By leveraging the BigFix Unified Management platform to help increase visibility, centrally manage all endpoints, and remediate issues identified on any managed asset, organizations can overcome compliance challenges while reducing costs. IT Operations and IT Security can leverage a unified assessment, remediation, and reporting tool to foster communication and ensure accuracy of reporting against compliance initiatives. And with scalability that ranges from one thousand to hundreds of thousands of endpoint systems, BigFix provides 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 security and 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. 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, Inc. BigFix and the BigFix Logo are registered trademarks of BigFix, Inc. Other trademarks, registered trademarks, and service marks are property oftheir respective owners. 2010202