

NONSTOP COMPLIANCE AT INFRASTRUCTURE SCALE: GO BEYOND COMPLIANCE TO PROACTIVE CONFIGURATION MANAGEMENT



Monitor compliance in real time via customized dashboards

ASSESS, RECONCILE, AND REMEDIATE

On a Single Endpoint or Enterprise-wide—From a Single Console

In addition to protecting against increasingly stealthy threats, companies need to harvest more and more granular data about their systems and security policies to prove compliance with regulatory standards. What drives many organizations to seek a configuration management solution is a failed audit that reveals 1) poor visibility into vulnerabilities in the system configuration and/or 2) a poorly managed or misconfigured system. Existing solutions present a multitude of problems, including manual audit, reporting, and remediation processes that are complex and expensive; long and painful cycles to address and fix configurations; and too many non-integrated point product silos offering too much disparate, uncorrelated data.

BigFix Security Configuration Management (SCM) brings verified real-time visibility, automated configuration remediation, and global scalability to the IT policies and standards compliance process. BigFix SCM is a comprehensive library of technical controls that help organizations achieve IT security compliance by detecting and enforcing security configuration policies using industry best practices and standards. SCM's policy libraries enable rapid implementation of compliance solutions conforming to individual customer requirements.

Product Benefits

- Continuously enforce security configuration baselines on hundreds of thousands of workstations, servers, and mobile devices worldwide—all from a single point of control
- Leverage security expertise and guidance provided by standards organizations to securely configure systems with compliance-based configuration checklists
- Report, remediate, and confirm remediation of any assets out of compliance in real time
- Obtain meaningful information on the health and security of all computers regardless of location, OS, connectivity (on or off the network), or applications installed, and enforce optimal use policies enterprise-wide
- Consolidate and unify the compliance lifecycle; reduce endpoint configuration and remediation times from days and weeks to minutes and hours

SYSTEM AND SERVER REQUIREMENTS

Supported Operating Systems for BigFix Server

- Windows 2000 Server SP 2+/2003/2008

Database Requirements for BigFix Server

- SQL Server 2000 SP4/2005

Supported Operating Systems for BigFix Console

Any of the following:

- Windows XP/2000/2003 Vista/2008

SUPPORTED OPERATING SYSTEMS

For BigFix Agent

All of the following:

- Windows
- Mac OS X
- Solaris
- IBM AIX
- IBM zLinux
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Red Hat Linux
- Fedora Linux

Note: Functionality may vary by supported platform. For an updated listing of supported OS versions, please see <http://support.bigfix.com>.

PRODUCT CERTIFICATIONS



Product Features

- Comprehensive “Always Current” view to cover all computing machines—even remote and mobile endpoints
- Single, centralized console view for real-time visibility into the current configuration posture of all endpoints
- Simple and easy-to-view Compliance Dashboard plus flexible ad-hoc query and reporting
- Ready-to-deploy checklists containing hundreds of standard configuration settings, mapped to industry standards and regulations such as Defense Information Systems Agency (DISA) and Security Technical Implementation Guides (STIG), among others; user can incorporate and change settings as needed
- Continuous closed-loop reconciliation to verify implementation or remediation of configuration changes
- SCAP certified for FDCC

Host-based vs. Scan-based Configuration Management

	Host-Based	Scan-Based
Data Depth	• Full, real-time access to information not provided through explicit system APIs	• Limited access to information not provided through explicit system APIs
Assessment and Enforcement	• Continuous assessment and automated enforcement of policies • Reduces the possibility of risk due to configuration drift • Assess/enforce on-network and off-network systems	• Periodic scanning provides only a snapshot in time • Introduces periods of increased risk due to lack of visibility • Can scan only what it sees on the corporate network
Network and System Requirements	• Virtually no performance impact to network—respond only with changes in configuration compliance as identified • Throttled to minimize system performance impact	• Scheduled in small batches to minimize overall network and system impact • Can significantly impact the system without the ability to throttle usage and assessment
Security Risk	• Solution co-exists with appropriate credentials and does not require special configuration to allow remote connection	• Requires external authentication and configuration to allow remote connectivity with privileged use

About BigFix

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.

©2009 BigFix, Inc. BigFix and the BigFix Logo are registered trademarks of BigFix, Inc. Other trademarks, registered trademarks, and service marks are property of their respective owners. 20090107