# IBM BigFix Compliance

*A single solution for managing endpoint security across the organization*

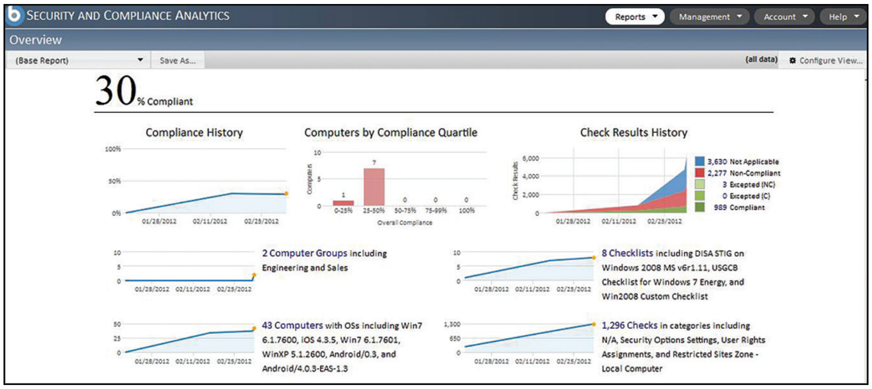
## Highlights

- Ensure continuous configuration compliance using thousands of out-of-the-box security controls based on industry best-practice security benchmarks with automated remediation and reporting
- Analyze and report on policy compliance status and trends and identify endpoint security exposure and risks
- Manage and distribute patches to all endpoints for a variety of operating systems and software applications
- Monitor and manage the status and health of various third party endpoint protection clients such as anti-virus and anti-malware tools
- Perform all security assessment, remediation, and reporting using a single multipurpose, intelligent agent on each endpoint
- Manage hundreds of thousands of endpoints, physical and virtual, regardless of location, connection type or status, all from a single management console

As the number of endpoints and the threats that can compromise them continue to grow at an unprecedented rate, IBM® BigFix® Compliance provides unified, real-time visibility and enforcement to protect complex and highly distributed environments.

Designed to ensure endpoint security across the organization, BigFix Compliance can help organizations both protect endpoints and meet security compliance standards. This easy-to-manage, quick-to-deploy solution supports security in an environment that is likely to include a large variety and large numbers of endpoints—from servers to desktop PCs, “roaming” Internet-connected laptops, smartphones and other mobile devices, as well as specialized equipment such as point-of-sale devices, ATMs and self-service kiosks.

BigFix Compliance can reduce the costs and complexity of IT management as it increases business agility, speed to remediation and accuracy. Its low impact on endpoint operations can enhance productivity and improve the user experience. By constantly enforcing policy compliance wherever endpoints roam, it helps reduce risk and increase audit visibility. Its intelligent agent’s speed and efficiency provides continuous compliance with automated audit cycles measured in minutes versus weeks.



2 Computer Groups including Engineering and Sales

8 Checklists including DISA STIG on Windows 2008 MS v6r1.11, USGCB Checklist for Windows 7 Energy, and Win2008 Custom Checklist

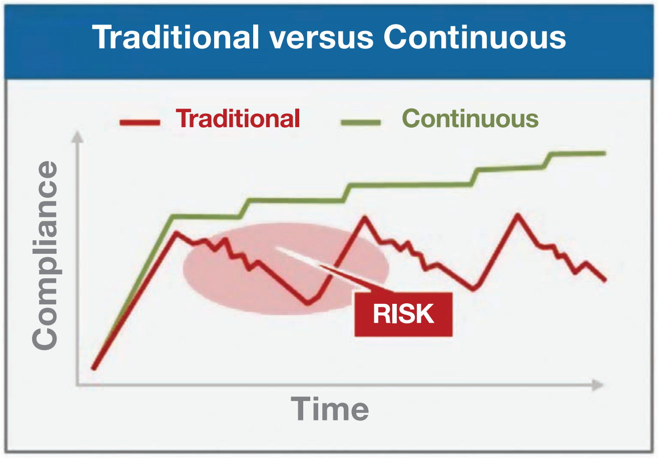
43 Computers with OSs including Win7 6.1.7600, iOS 4.3.5, Win7 6.1.7601, WinXP 5.1.2600, Android/0.3, and Android/4.0.3-EAS-1.3

1,296 Checks in categories including N/A, Security Options Settings, User Rights Assignments, and Restricted Sites Zone - Local Computer

IBM BigFix Compliance provides detailed analytics that help organizations visualize the effectiveness of security and compliance efforts.

## Addressing security needs across the organization

BigFix Compliance addresses security challenges associated with desktop, server, mobile and distributed environments. By providing unified endpoint management and security, it helps ensure continuous protection and compliance. For example, it can dramatically shrink gaps in security exposures by applying software patches in minutes. And it can help bridge the gap between functions such as those establishing and executing strategy and policy, those managing devices in real time, and those generating reports on security and compliance issues. Continuous configuration monitoring and remediation can avoid compliance drift, by including this powerful diagram:



The capabilities of BigFix Compliance include:

- Providing accurate, precise and up-to-the-minute visibility into and continuous enforcement of security configurations and patches
- Centralizing management of third-party anti-malware and firewall protection
- Automatically assessing and remediating security policy configurations using best-practice checklists based on security benchmarks published by Center for Internet Security (CIS), US Government Configuration Baseline (USGCB) and Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)
- Supporting Security Content Automation Protocol (SCAP); IBM BigFix is also the first product certified by the National Institute of Standards and Technology (NIST) for both assessment and remediation
- Securely transmitting endpoint instructions as demonstrated through National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) EAL3 and Federal Information Processing Standards (FIPS) 140-2, Level 2 certifications
- Supporting the Open Vulnerability and Assessment Language (OVAL) standard to promote open and publicly available security content
- Receiving and acting on vulnerability and security risk alerts published by the NIST National Vulnerability Database
- Showing trends and analysis of security configuration changes through advanced analytics
- Using analytics to provide insight and reporting to meet compliance regulations and IT security objectives, including determining progress and historical trends toward continuous security configuration policy compliance, identifying endpoint security exposures and risks, and more

Additional capabilities provided by IBM BigFix include:

- Discovering endpoints of which organizations may not be aware—up to 30 percent more, in some cases
- Providing a single console for management, configuration, discovery and security functions, which simplifies operations
- Targeting specific actions to an exact type of endpoint configuration or user type using virtually any hardware or software property
- Employing a unified management infrastructure to coordinate among IT, security, desktop and server operations
- Reaching endpoints regardless of location, connection type or status with comprehensive management for all major operating systems, third-party applications and policy-based patches

BigFix Compliance enables automated, highly targeted processes that provide control, visibility and speed to affect change and report on compliance. Possessing a near real-time, organization-wide analysis and action tool such as BigFix is indispensable when responding to advanced zero-day threats. With BigFix, the remediation cycles are short and fast, which enables an industry-leading, rapid-response capability for addressing malware and security exposures.

## Delivering a broad range of powerful security functions

BigFix Compliance includes the following key functions, while enabling users to easily add other targeted functions as needed—without added infrastructure or implementation costs.

### Patch management

Patch management includes comprehensive capabilities for delivering patches for Microsoft Windows, UNIX, Linux, and Mac OS as well as third-party application vendors to distributed endpoints—regardless of location, connection type or status. A single management server can support up to 250,000 endpoints, shortening times for patches with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks. Real-time reporting provides information on which patches were deployed, when they were deployed and who deployed them, as well as automatic confirmation that patches were successfully applied for a complete closed-loop solution to the patching process.

### Security configuration management

Validated through NIST, the solution's security configuration features provide a comprehensive library of technical controls that can help you achieve security compliance by detecting and enforcing security configurations. Policy libraries support continuous enforcement of configuration baselines; report, remediate and confirm remediation of noncompliant endpoints in real time; and ensure a verified real-time view of all endpoints.

This feature delivers meaningful information on the health and security of endpoints regardless of location, operating system, connection (including wired computers or intermittently connected mobile laptops), or applications installed. It helps consolidate and unify the compliance lifecycle, reducing endpoint configuration and remediation times.

### Payment Card Industry Data Security Standard (PCI-DSS) compliance

The BigFix Compliance Payment Card Industry (PCI) Add-on is designed to help with the enforcement and compliance reporting needed to satisfy the latest PCI-DSS requirements. Specific PCI-DSS configuration and policy compliance checks, as well as specialized dashboards, simplify the monitoring and reporting of PCI compliance, and the capability to continuously and automatically manage system configuration and currency improves endpoint security and integrity. Together, these capabilities help to protect organizations from the malicious or unintentional loss of confidential customer and financial information while lowering operational and security administration costs. This helps avoid the negative press, and the legal and financial headaches, that a payment card data breach would likely generate.

### Vulnerability management

Vulnerability management provides vulnerability discovery and assessment to identify vulnerabilities on endpoints and prevent them from being exploited. This feature assesses Windows systems against standardized OVAL vulnerability definitions and reports on detected vulnerabilities based on severity in real-time. The result provides enhanced visibility to security posture and enables full integration at every step in the entire discover-assess-remediate-report workflow.

With this capability, IT staff can identify and eliminate known vulnerabilities across endpoints. BigFix Compliance includes automated feeds from vulnerability checklists such as the NIST National Vulnerability Database. By using a single tool to both discover and report vulnerabilities, administrators can increase speed and accuracy, helping shorten remediation cycles for patch deployment, software updates and vulnerability fixes. Administrators can set alarms to quickly identify rogue assets and take steps to locate them for remediation or removal. They can also extend security management to mobile clients on or off the network.

### Asset discovery

With BigFix Compliance, asset discovery is no longer a snapshot counting exercise. Instead, it creates dynamic situational awareness about changing conditions in the infrastructure. The ability to scan the entire network frequently delivers pervasive visibility and control to help ensure that organizations quickly identify all IP-addressable devices—including virtual machines, network devices and peripherals such as printers, scanners, routers and switches, in addition to computer endpoints—with minimal network impact. This function helps maintain visibility into all endpoints, including mobile laptop and notebook computers that are roaming beyond the organization's network.

### Endpoint Inspection

BigFix Query provides a real-time status of all your endpoints, enabling accurate identification and inspection of vulnerable devices through a user friendly web interface. You can interrogate endpoints and get precise answers back in seconds, telling you which policies are enforced and which applications and services are installed. You can even examine files and system configuration settings to help you identify additional security threats. Users can use a library of pre-defined queries or quickly and easily create their own custom queries. BigFix Query also verifies the remediation of endpoints, helping to bridge the gap between security and IT operations.

### Multivendor endpoint protection management

This feature gives administrators a single point of control for managing third-party endpoint security clients from vendors such as Computer Associates, McAfee, Sophos, Symantec and Trend Micro. With this centralized management capability, organizations can enhance the scalability, speed and reliability of protection solutions. This feature monitors system health to ensure that endpoint security clients are always running and that virus signatures are updated. In addition to providing a unified view of disparate technologies, it facilitates migrating endpoints from one solution to another with "one-click" software removal and reinstall. Closed-loop verification ensures that updates and other changes are completed, including Internet-enabled verification for endpoints disconnected from the network.

BigFix Compliance also integrates with IBM BigFix Protection to protect physical and virtual endpoints from damage caused by viruses, Trojan horses, worms, spyware, rootkits, web threats and their new variants. This can help reduce business disruptions that can result from endpoint infection, identity theft, data loss, network downtime, lost productivity and compliance violations.

## Network self-quarantine

BigFix Compliance automatically assesses endpoints against required compliance configurations—and if a Windows endpoint is found to be out of compliance, the solution can configure the endpoint so that it is placed in network quarantine until compliance is achieved. BigFix retains management access to the endpoint, but all other access is disabled.

## Accurate and actionable insight

BigFix integrates with IBM QRadar® Security Intelligence Platform to provide better endpoint intelligence as a key component of organization-wide intelligence about security vulnerabilities. BigFix can help:

- Increase the QRadar vulnerability database accuracy, improving security incident and risk analytics and limiting potential vulnerabilities
- Establish a security baseline for endpoints and improve alerting on variations to detect threats that other security solutions might miss
- Take vulnerabilities identified and prioritized by the QRadar platform, provide remediation actions (applying patches, quarantine, etc.) and send action status back to QRadar to form a real closed-loop security risk management cycle.

### IBM BigFix Compliance at a glance

**Server requirements:**
- Microsoft SQL Server 2005, 2008, 2012
- Microsoft Windows Server 2003, 2008, 2008 R2, 2012
- IBM DB2® v10.1
- Red Hat Enterprise Linux v6

**Console requirements:**
- Windows XP, 2003, Vista, 2008, 2008 R2, 7, 8, 2012

**Supported platforms for the agent:**
- Windows XP, 2000, 2003, Vista, 2008, 2008 R2, 7, 8, 2012, CE, Mobile, XP Embedded, Embedded Point-of-Sale
- Mac OS X
- Solaris
- IBM AIX®
- Linux on IBM z Systems™
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- CentOS Linux
- Debian Linux
- Ubuntu Linux

## The IBM BigFix family

Organizations can realize significant value by deploying additional products from the BigFix family, beyond BigFix Compliance. The broader BigFix family addresses the convergence of system management and security requirements by delivering capabilities for mobile device management, asset discovery, inventory, software distribution, operating system deployment, software usage analysis and more. Because IBM designed the products so that all functions operate from the same console, management server and single intelligent agent, adding more services is a simple matter of a license key change.

### IBM BigFix technology

The power behind all BigFix functions is a unique, single-infrastructure approach that distributes decision-making out to the endpoints, providing extraordinary benefits across the entire solution family, with features that include:

- **Intelligent agent—**BigFix places an intelligent agent on each endpoint to perform multiple functions, including continuous self-assessment and policy enforcement—with minimal impact on system performance.
- **Reporting—**The single, unified console built into BigFix orchestrates a high level of visibility that includes real-time and continuous reporting and analysis from the intelligent agent.
- **Relay capabilities—**The scalable and lightweight BigFix architecture allows any agent to be configured as a relay between other agents and the console. This function enables the use of existing servers or workstations to transfer packages across the network, reducing the need for servers.
- **IBM Fixlet® messages—**The Fixlet Relevance Language is a published command language that enables users, business partners and developers to create custom policies and services for endpoints managed by BigFix solutions.

## Why IBM?

IBM BigFix Compliance is part of the comprehensive IBM security portfolio, helping address security challenges across the organization. Supporting the instrumented, interconnected and intelligent IT operations of a smarter planet, IBM security solutions help ensure real-time visibility, centralized control and enhanced security for the entire IT infrastructure, including its globally distributed endpoints.

## For more information

To learn more about IBM BigFix Compliance, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/ibm-bigfix-compliance

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Please Recycle