HCL SOFTWARE | BIGFIX

HCL

BigFix Compliance

A single solution for managing endpoint security across the organization

As the number of endpoints and the threats that can compromise them continue to grow at an unprecedented rate, 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, and "roaming" Internet-connected laptops, as well as specialized equipment such as point-of-sale devices, ATMs and self-service kiosks.

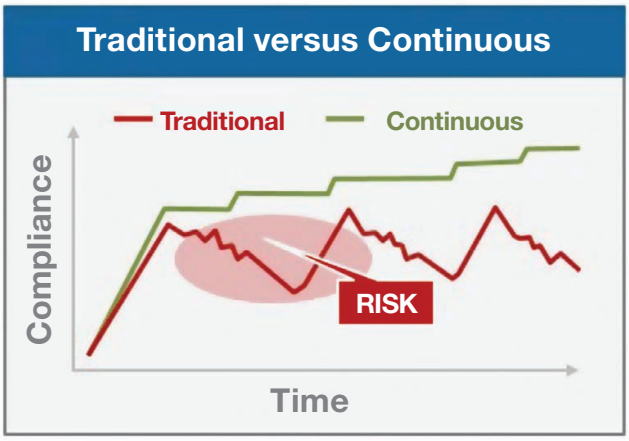
BigFix Compliance can reduce the costs and complexity of IT management as it increases business agility, speed to remediation and accuracy. Its low impact on endpoint operations can enhance productivity and improve the user experience. By constantly enforcing policy compliance wherever endpoints roam, 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.

Highlights

- Ensure continuous configuration compliance using thousands of out-of-the-box security controls based on industry best-practice security benchmarks with effective remediation of configuration drifts
- Analyze and report on policy compliance status and historical trends to assess endpoint security risks and evaluate compliance effort effectiveness
- Manage and distribute patches to all end- points for a variety of operating systems and software applications
- Track and report on patching activity status and historical trend to assess security posture and demonstrate compliance progress
- Monitor and manage the deployment status and health of various third party endpoint protection solutions such as anti-virus and anti-malware tools
- Assess Windows endpoints against standardized, OVAL based security vulnerability definitions to report vulnerabilities more efficiently
- Quarantine endpoints that are out of compliance to minimize risk of compromised endpoints contaminating the network
- Provide PCI DSS specific checklists, dashboards, and report to accelerate achieving PCI compliance

Addressing security needs across the organization

BigFix Compliance addresses security challenges associated with desktop, server, mobile and distributed environments. By providing comprehensive 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.



BigFix Compliance capabilities:

- Providing current and accurate visibility into and continuous enforcement of security configurations and patches
- Centralizing management of third-party anti-virus software and signatures
- Automatically assessing and remediating security policy configurations using best-practice checklists based on security benchmarks such as the Payment Card Industry Data Security Standard (PCI DSS), 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); HCL BigFix is also the first product certified by the National Institute of Standards and Technology (NIST) for both assessment and remediation
- Supporting the Open Vulnerability and Assessment Language (OVAL) standard to promote open and publicly available security content
- 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 objectivves, including determining progress and historical trends toward continuous security configuration policy compliance, identifying endpoint security exposures and risks.
- Integrate with third party vulnerability management solutions to pull prioritized vulnerabilities related to available patches in BigFix in a single dashboard view
- Quarantine systems through the BigFix agent itself, isolating the target the network while maintaining control and visibility through the BigFix agent in order to remediate and fix.

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 without adding additional infrastructure or implementation costs:

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.

Patch management

Patch management includes comprehensive capabilities for delivering patches for Windows, UNIX, Linux and MacOS and for third-party applications, including Adobe, Mozilla, Apple and Java, to distributed endpoints—regardless of their location, connection type or status. A single management server can support up to 250,000 endpoints, shortening patch times with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks. Virtual patch management capabilities enable off line patching, making stale virtual machine images a thing of the past. 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 applied, for a complete closed-loop solution to the patching process.

Security configuration management

BigFix Compliance 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.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.

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.

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 to choose the right technology for their environment.

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.

Integration

BigFix can integrate with other IT Security solutions extending functionality and improving staff productivity. For example, BigFix integrates with SIEM solutions such as QRadar and Splunk, EDR solutions such as Carbon Black and CyFIR, and Vulnerability managers such as Rapid 7, Tenable, Forescout, and CISCO AMP.

The BigFix family

You can further consolidate tools, reduce the number of end-point agents and lower your management costs by extending your investment in BigFix Compliance to include other modules in the BigFix family. Because all functions operate from the same console, management server and endpoint agent, adding more services is a simple matter of a license key change. The BigFix family includes:

- BigFix Lifecycle—This easy-to-manage, quick-to-deploy solution provides unified, real-time visibility and management of endpoints including asset discovery, patch management, software distribution, operating system deployment, and remote desktop control.
- BigFix Inventory—This software enables users to discover and analyze applications installed on desktops, laptops and servers. Drill-down information about software publishers, titles and applications—down to the version level—also includes aggregated statistics and usage information.

BigFix Compliance at a glance

Server requirements

- Microsoft SQL Server 2005/2008/2012
- Microsoft Windows Server 2003/2008/2008 R2/2012
- 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
- Solaris
- IBM AIX
- Linux on z Systems™
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- CentOS Linux
- Debian Linux
- Ubuntu Linux

Built on 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. Features include:

- An intelligent agent—BigFix utilizes an industry-leading approach that places an intelligent agent on each endpoint. This single agent performs multiple functions including continuous self-assessment and policy enforcement—yet has minimal impact on system performance. In contrast to traditional client-server architectures that wait for instructions from a central control point, this agent initiates actions in an intelligent manner, sending messages upstream to the central management server and pulling patches, configurations or other information to the endpoint when necessary to comply with a relevant policy. As a result, the central management server always knows the compliance and change status of endpoints, enabling rapid and up-to-date compliance reporting.
- Reporting—The single, unified console built into BigFix orchestrates a high level of visibility that includes real-time continuous reporting and analysis from the intelligent agents on an organization's endpoints.
- Relay capabilities—The scalable and lightweight architecture of BigFix allows any agent to be configured as a relay between other agents and the console. This relay function enables the use of existing servers or workstations to transfer packages across the network, reducing the need for servers.
- Fixlet® messages—The Fixlet Relevance Language is a published command language that enables customers, business partners and developers to create custom policies and services for endpoints managed by BigFix solutions.

For more information

To learn more about BigFix, contact your HCL Software representative, HCL Business Partner, or visit **www.BigFix.com.**

About HCL Software

HCL Software is a division of HCL Technologies that develops and delivers a next-generation portfolio of enterprise-grade software-based offerings with flexible consumption models, spanning traditional on-premises software, Software-as-a-Service (SaaS), and bundled managed services. We bring speed, insights and innovations (big and small) to create value for our customers. HCL Software areas include DevOps, Security, Automation, Application Modernization, Data and Integration Infrastructure, and several Business Applications. HCL embraces the real-world complexity of multi-mode IT that ranges from mainframe to cloud and everything in between while focusing on customer success and building 'Relationships Beyond the Contract.

HCL Corporation Pvt. Ltd.
Corporate Towers,
HCL Technology Hub,
Plot No 3A, Sector 126,
Noida - 201303. UP (India)

Produced in the United States of America.

wx10549 v1.2