HCL SOFTWARE | BIGFIX

HCL

BigFix Compliance

Ensuring continuous compliance of security and regulatory policies

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 policy 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 requirements and policies. This easy-to-manage,quick-to-deploy solution supports security in an environment that is likely to include a large variety and largenumbers of endpoints—from servers to desktop PCs, and “roaming” Internet-connected laptops, as well asspecialized 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 user experience. By constantly enforcing policy compliance wherever endpoints roam, it helps reduce risk and increase audit visibility. Its intelligent agent’s speed and e!ciency provide 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 such as CIS and DISA STIG, with effective remediation of configuration drifts
- Manage and distribute patches to all endpoints for a variety of operating systems and software applications
- Track, analyze and report on policy compliance status and historical trend, across three key security domains including security configuration, patch, and vulnerability, to assess endpoint security risk 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
- Quarantine endpoints that are out of compliance to minimize the risk of compromised endpoints contaminating the network

Addressing security needs across the organization

BigFix Compliance addresses security challenges associated with the desktop, server, mobile laptop, 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 monitoring security configurations and remediate configuration drifts in minutes. It can effectively help bridge the gap among various functions such as those establishing and executing security strategy and policy, those managing devices in real-time, and those generating reports on security and compliance issues.

Continuous Compliance Reduces Risk

BigFix Compliance capabilities

BigFix Compliance provides many important capabilities which include:

- Providing a real-time and automatic assessment to security configurations, continuous enforcement of security policies, and effective remediation of configuration drifts
- Supporting out-of-the-box security checklists based on industry best-practice security benchmarks such as the Payment Card Industry Data Security Standard (PCI DSS), Center for Internet Security (CIS), and Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)
- Managing and distributing patches to all endpoints for a variety of operating systems and software applications
- Tracking, analyzing and reporting on policy compliance status and historical trends, across three key security domains — security configuration, patch, and vulnerability — to assess endpoint security risk and demonstrate compliance progress
- Monitoring and managing the deployment status and health of various third-party endpoint protection solutions such as anti-virus and anti-malware tools
- Scanning the entire network for all IP-addressable devices to discover any endpoints that are not managed by BigFix
- Interrogating endpoints with a Query tool and pre-defined or user-created queries and get precise answers back in seconds
- Quarantining 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
- Integrating with other market leading security solutions to provide deeper endpoint intelligence, identity risks, and remediate vulnerabilities more effectively.

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:

Device Discovery

With BigFix Compliance, device 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 offline 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

Out of the box, BigFix Compliance provide an extensive list of checklists developed based on authoritative security benchmarks published by CIS, DISA STIG, USGCB, PCI DSS. The checks in a checklist can be easily customized to support an organization's security policy. Once a checklist is applied to an endpoint, BigFix continually evaluates the endpoint's security configurations against the deployed checklist. Compliance status is also continually collected and reported to BigFix Server. Any 'configuration drift' can be identified quickly and an administrator can remediate the configuration issue remotely. With such a powerful approach of monitoring, reporting, and remediating security configurations across the entire IT environment, an organization can enforce endpoint security policies, minimize security risks, and effectively reduce endpoint management costs.

BigFix Compliance provides security configuration management for more than 60 operating systems and applications. Checklists are constantly refreshed based on the latest published benchmarks to provide optimal endpoint protection for organizations

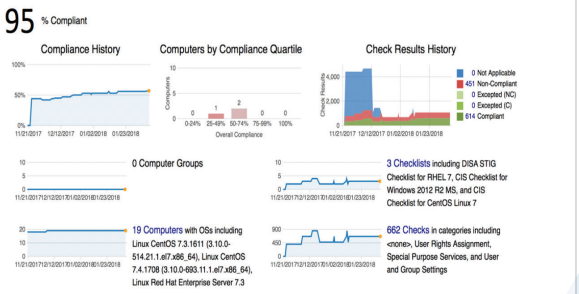
Compliance analytics

The compliance statuses of all endpoints against deployed policies are continually collected, aggregated, and reported using a powerful Compliance Analytics engine, database and user interface in BigFix Compliance. Various compliance reports, showing both current status and historical trend for the entire deployment or individual endpoint, provide comprehensive analytics to meet the various needs of security, IT operation, or compliance teams. With Compliance Analytics, an organization is able to can track the effectiveness of its compliance effort and quickly identify security exposures and risks.

Compliance Analytics provides consistent reports across all three security domains: Security configuration, Patch and Vulnerability.

Security configuration reporting

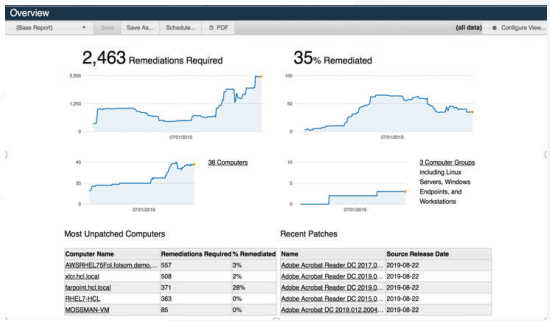
For all the security configuration checklists deployed across the entire environment using BigFix Compliance, Compliance Analytics provides various reports to show both current status and historic trend for individual endpoint, individual checklist, or even individual check. An aggregated compliance posture for the entire deployment is also provided to report the overall status and progress toward the desired security configuration policies.



Security Configuration Reporting

Patch reporting

Patch reporting extends the analytics and reporting capabilities of BigFix Compliance from security configuration to security patching. This feature allows an organization to gain a comprehensive and historical view of patching activities across the entire deployment to assess the overall patching posture. It can enable more efficient prioritization of vulnerability remediation by identifying the critical and high severity patches that are yet to be applied. It also tracks when each patch is released and applied to each endpoint to help organizations demonstrate compliance with regulations/policies and pass audits.

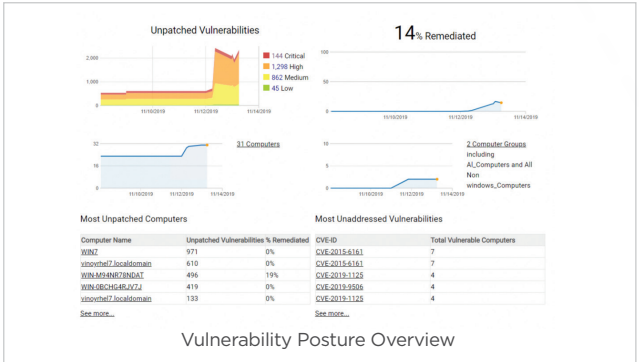


Patch Reporting

Vulnerability reporting

BigFix Compliance Vulnerability Reporting, new in BigFix 10, focuses on tracking and reporting of endpoints' vulnerability posture as a result of patching actions, enabling organizations to more broadly identify risks and demonstrate compliance. This vulnerability reporting feature provides significant values to multiple teams:

- **Risk Posture Assessment:** A Security Operations Center Manager or Security Analyst can get the current status, historical trend and details of vulnerabilities of various severities existed on each endpoint or across the environment.
- **Remediation Task Prioritization:** An IT Operations Specialist can get more information to help him more effectively prioritize his patching actions to maximize the impact to the vulnerability posture change.
- **Vulnerability Compliance Demonstration:** A Compliance Specialist can report how vulnerabilities have been remediated by patching actions to demonstrate compliance with specific regulatory or organization policies.



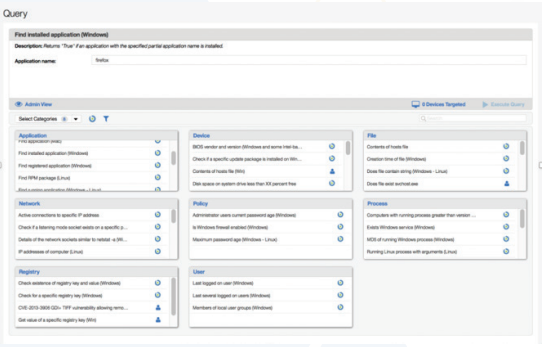
Vulnerability Posture Overview

Quarantine of non-compliant systems

Many organizations desire to strictly control how endpoints can access the corporate' intranet, based on endpoints' status or configurations against a pre-defined policy. For example, an endpoint cannot access the intranet unless it has the latest security patch installed or has the latest virus definition used by its anti-virus tool. BigFix Compliance provides a self-quarantine capability, so if an endpoint is found to be out of compliance with an endpoint compliance policy, the endpoint is placed in network quarantine until its compliance is achieved. A quarantined endpoint still has a connection to the BigFix infrastructure (in order to be remediated), but all other network accesses are disabled.

Endpoint inspection

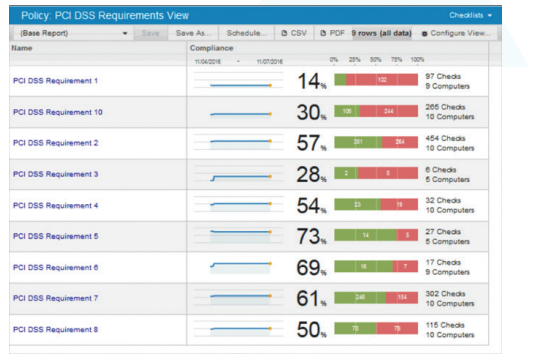
BigFix Query provides real-time status of all your endpoints, enabling accurate identification and inspection of vulnerable devices through a user-friendly web interface. You can interrogate endpoints and get precise answers back in seconds, telling you which policies are enforced and which applications 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.



BigFix Query

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

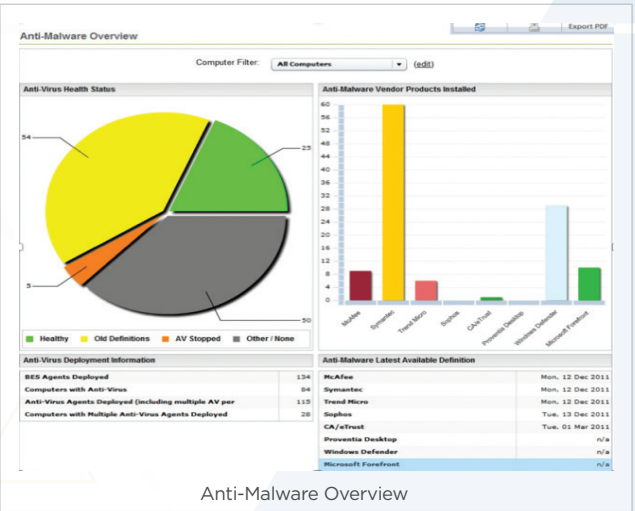
The BigFix Compliance Payment Card Industry (PCI) Add-on is designed to help with the enforcement and compliance reporting needed to satisfy the latest PCI-DSS requirements. Specific PCI-DSS configuration and policy compliance checks, as well as specialized dashboards, simplify the monitoring and reporting of PCI compliance, and the capability to continuously and automatically manage system configuration and currency improve 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.



Example PCI DSS Requirement Compliance

Multivendor endpoint protection management

This feature gives administrators a single point of control for managing third-party endpoint security clients from vendors such as McAfee, Symantec, Trend Micro, Sophos, and Microsoft. 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 reinstalls. Closed-loop verification ensures that updates and other changes are completed, including Internet-enabled verification for endpoints disconnected from the network.



Anti-Malware Overview

Integration

BigFix is integrated with other IT security solutions to extend its functionalities and provide deeper endpoint intelligence, identity risks, and remediate vulnerabilities more effectively. For example, BigFix is tightly integrated with Security Information and Event Management (SIEM) solutions such as IBM QRadar; Endpoint Detection and Response (EDR) solutions such as Carbon Black; and Network Access Control (NAC) solutions such as Forescout.

The BigFix Family

By extending your investment in the BigFix family, you can further consolidate tools, reduce the number of endpoint agents, and lower your management costs. 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 Inventory**—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 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, power management, and remote desktop control.
- **BigFix Insights**—New with BigFix 10, BigFix Insights enables teams to quickly report their organization’s threat posture to executives and perform advanced analysis to drive next steps. This new offering provides a powerful endpoint Data Lake and integration platform for deeper data insights across traditional on-premise, cloud, and MDM API managed endpoints. Insights leverages Business Intelligence (BI) reporting tools to provide provides out-of-the-box and customizable reports.
- **Modern Client Management** —New with BigFix 10, you can manage Windows 10 and MacOS endpoints, where a BigFix Agent is not installed, by leveraging a Mobile Device Management Application Programming Interface (MDM API) approach. Modern Client Management provides the ability to manage both modern and traditional endpoints using a single tool. Features in BigFix 10 include end-user-initiated enrollment, detailed inventory of endpoints, and a number of MDM actions such as remote wipe.

Why BigFix?

BigFix is built on a unique, highly scalable infrastructure that distributes decision making out to the endpoints. This provides extraordinary functional and performance benefits across the entire BigFix family while reducing the cost of endpoint management and infrastructure complexity. BigFix features:

- **A single intelligent agent**—The BigFix Agent performs multiple functions, including continuous self-assessment and policy enforcement, with minimal impact on system performance. The BigFix 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 in real-time. The BigFix Agent runs on more than 90 operating systems across Microsoft Windows, Linux, UNIX, and MacOS.
- **BigFix Fixlets™**—BigFix Fixlets are small units of automation that allow IT Teams to simplify their daily operations and focus on more complex operations. BigFix provides more than 500,000 Fixlets out of the box. The BigFix team is continuously updating the Fixlet library, with over 130 content updates a month. BigFix users, business partners, and developers can leverage Fixlets to create custom policies and services for endpoints managed by BigFix. A community library of Fixlets is available on BigFix.me.
- **Highly scalable architecture**—A single BigFix Management Server can manage up to 250,000 physical and virtual computers, over private or public networks. Managed endpoints may include servers, desktops, roaming laptops, and specialized devices such as Point-Of-Sale (POS) devices, ATMs, and self-service kiosks.
- **Multicloud support**—Cloud endpoints can be easily discovered and viewed alongside traditional endpoints, in a single user interface, with BigFix 10. Knowing what you have is half the battle, and BigFix 10 allows you to go a step further and deploy the BigFix Agent for complete visibility, control, and security of these endpoints. It allows you to manage endpoints running in multiple cloud environments simultaneously – such as Amazon Web Services (AWS), Microsoft Azure, and VMWare – alongside

HCL

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.