HCL SOFTWARE | BIGFIX

HCL

BigFix Compliance

Ensuring continuous compliance of security and regulatory policies

The number of security threats that compromise endpoints and cause business level damages have been continually growing. With an ever more mobile workforce and new cloud initiatives, the very nature of the endpoint is changing. Along with it, heightened regulatory concerns put additional burdens on over stretched IT groups.

BigFix® Compliance provides unified, real-time visibility and policy enforcement to protect complex, highly distributed environments. Designed to dramatically reduce compliance reporting overhead as well as enforce compliance to standards, BigFix Compliance can help organizations both protect endpoints and meet security compliance requirements and policies.

This easy-to-manage, quick-to-deploy solution supports compliance initiatives for highly diverse environments —from servers to desktop PCs, mobile Internet-connected laptops, virtual servers, cloud based systems, as well as specialized equipment such as point-of-sale devices, ATMs and self-service kiosks. 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 efficiency provide continuous compliance with automated audit cycles measured in minutes versus weeks.

Highlights

- Continuously enforce compliance to industry security benchmarks or standards such as CIS, DISA STIG and PCI for endpoints virtually running any OS, in any location with automatic remediation of configuration drifts back to compliance baselines
- Over 20,000 out-of-the-box compliance checks are continuously updated to current standard, which dramatically reduces the need for compliance expertise and the effort to put all endpoints in compliance.
- Track and report compliance historical trends across security configuration, patch and vulnerability, to assess endpoint security risk and demonstrate compliance progress over time
- Monitor and manage the deployment status and health of leading third-party Endpoint Protection solutions
- Manage and distribute patches to all endpoints, regardless of OS, location, connection and type
- Support compliance controls for Windows 10 and macOS clients without agents via BigFix Modern Client Management
- Speed vulnerability remediation by automating the manual correlation of vulnerability data from external sources with BigFix Insights for Vulnerability Remediation.

Continuous Compliance

BigFix's continuous compliance technology virtually eliminates visibility and compliance gaps. Continuous compliance puts rules and enforcement at the endpoint and loops through all assigned polices without pausing, ensuring the endpoint is always in a compliant state.

In contrast, traditional point-in-time management solutions "check in" at unpredictable times, reducing viability, creating gaps and increased risk due to noncompliant systems. These gaps can be caused by:

- Disconnected endpoints which are off network
- Critical patches released on Patch Tuesday may take days or weeks to deploy and validate
- Complete patch status reporting may take days or weeks
- End user-initiated changes effecting security compliance

Because of continuous compliance, BigFix can commonly deliver 99% compliance across the enterprise.

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 -- all supporting continuous compliance of self-healing endpoints across more than 60 operating systems and applications.
- 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.
- 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 predefined or user-created queries and get precise answers back in seconds.
- Quarantining systems through the BigFix agent itself, isolating the target from the network while maintaining control and visibility through the BigFix agent for remediation.
- Integrating with other market leading security solutions to provide deeper endpoint intelligence, identify risks, and remediate vulnerabilities more effectively.

Having a near real-time, visibility across the organization, BigFix is indispensable when combating zero-day threats. With BigFix, the remediation cycles are short and fast, which enables an industry-leading, rapid-response for address Security issues.

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 vendors, including Adobe, Mozilla, Apple, and Oracle, 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

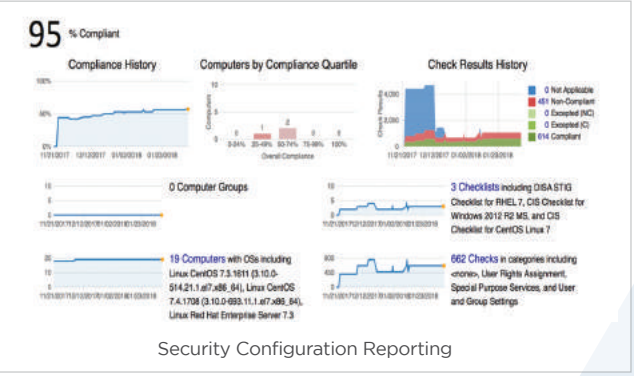
Out of the box, BigFix Compliance provide an extensive list of checklists developed based on authoritative security benchmarks published by CIS, DISA STIG, USGCB, PCI DSS. The checks in a checklist can be easily customized to support an organization's security policy. Once a checklist is applied to an endpoint, BigFix continually evaluates the endpoint's security configurations against the deployed checklist. Compliance status is also continually collected and reported to the 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.

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 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

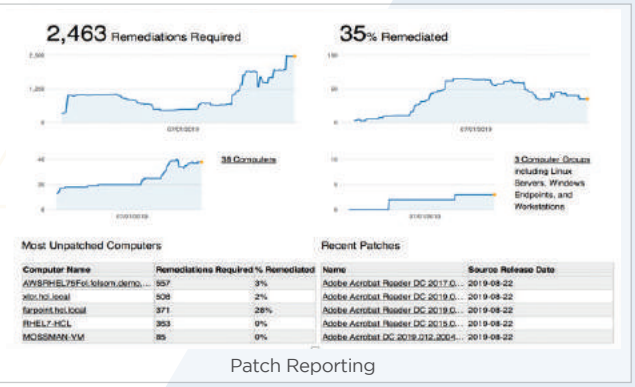
For all the security configuration checklists deployed across the entire environment using BigFix Compliance, Compliance Analytics provides various reports to show both current status and historic trend for individual endpoint, individual checklist, or even individual check. An aggregated compliance 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

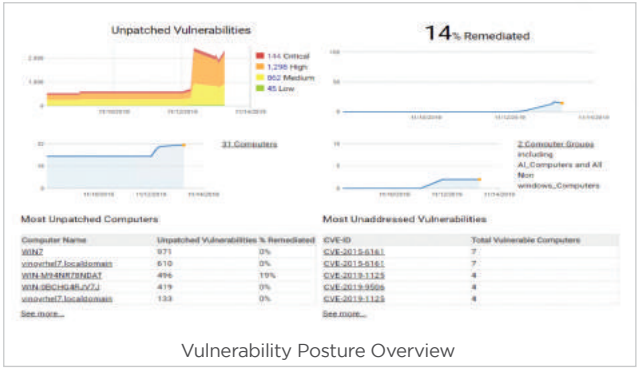


Patch Reporting

Vulnerability reporting

BigFix Compliance Vulnerability Reporting 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 value to the organization by providing:

- **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 more effectively prioritize 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

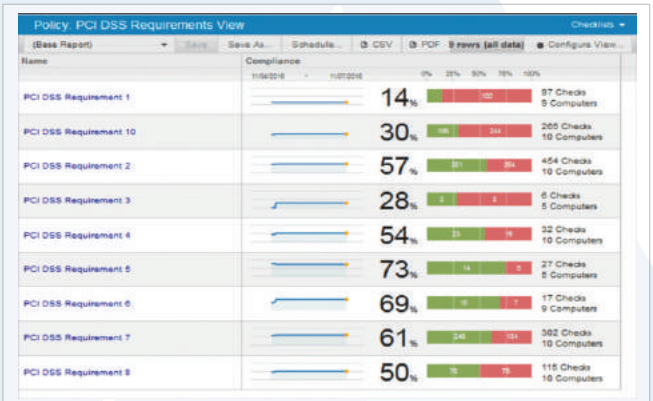
Many organizations need to strictly control how endpoints can access the corporate intranet, based on endpoint status or configuration against a predefined policy. For example, an endpoint cannot access the intranet unless it has the latest security patch installed or has the latest virus definition used by its anti-virus tool. BigFix Compliance provides a self-quarantine capability, so if an endpoint is discovered to be out of compliance with an endpoint compliance policy, the endpoint is placed in network quarantine until compliance is achieved. A quarantined endpoint can still be managed by BigFix so that it can be remediated, but all other network access is 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 predefined 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.

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 can protect organizations from the malicious or unintentional loss of confidential customer and financial information while lowering operational and security administration costs. This can prevent the negative publicity, legal and financial impacts of a payment card data breach.



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.

Analytics and reporting

Organizations need to quickly report their organization's threat posture to executives and perform advanced analysis to drive next steps. BigFix Insights provides a powerful endpoint and integration platform and database for deeper data insights across traditional on-premise, cloud, and MDM API managed endpoints. BigFix Insights leverages Business Intelligence (BI) reporting tools to provide out-of-the-box and customizable reports. BigFix Insights is included with BigFix Compliance.

Vulnerability remediation

Currently it can take days or weeks for IT Operations to remediate vulnerabilities after a vulnerability scan, exposing organizations to potential attacks. BigFix Insights for Vulnerability Remediation automates the typically manual correlation of vulnerability data from Tenable or Qualys with remediation Fixlets available within BigFix. Using BigFix Insights for Vulnerability Remediation, organizations can speed remediation of endpoint vulnerabilities across the enterprise by compressing the time from vulnerability assessment to remediation; dramatically reduce errors from spreadsheet-based, manual processes; and improve an enterprise's security posture by reducing the attack surface across the fleet of endpoints. BigFix Insights for Vulnerability Remediation is included with BigFix Compliance.

Modern client management

Organizations are deploying Windows 10 and macOS endpoints across the enterprise at an accelerated pace. Both operating systems are capable of being managed using either a traditional agent or Mobile Device Management (MDM) APIs. Leveraging both approaches together provides the greatest range of management and automation capabilities. BigFix Modern Client Management allows organizations the ability to manage both modern and legacy endpoints side-by-side using a single, enterprise endpoint management solution. BigFix Modern Client Management is included with BigFix Compliance.

Integration options

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.

Prerequisites

The prerequisites for BigFix Compliance are available online at help.hcltechsw.com/bigfix/landing/index.html.

Why BigFix?

The HCL BigFix endpoint management platform helps IT Operations with Continuous Compliance and Intelligent Automation to manage over 100 operating system versions, enabling streamlined management processes, tool consolidation and operational cost reduction.

Unlike complex tools that cover a limited portion of endpoints, the unified architecture of BigFix can effectively manage and ensure compliance of all servers, desktops, and mobile devices whether they are in the office, at home or in the cloud. BigFix can find and fix endpoints faster than any other solution – delivering greater than 98% first-pass patch success rates.

BigFix integrates with leading vulnerability management solutions like Tenable and Qualys to dramatically reduce the time required to remediate vulnerabilities. It also extends its well-established endpoint management capabilities to AWS, Azure, and Google clouds, enabling organizations to use a single solution to manage multiple clouds and on-prem in a consistent manner.

The unique approach of BigFix, coupled with thousands of out-of-the-box security checks, will enhance your security posture and automate the fight against ransomware and other cyberattacks.

The BigFix Family

BigFix is the only endpoint management platform that enables IT operations and security teams to fully automate the discovery, management and remediation of vulnerabilities and assets – for every endpoint, whether its on-prem, virtual, cloud or mobile– regardless of operating system, location or connectivity.

BigFix empowers businesses and organizations to find more, fix more and do more, faster.

The BigFix family includes:

- **BigFix Lifecycle** to automate endpoint lifecycle management by enabling software and operating system deployment, continuous compliance, self-service software catalog, power management, server automation, and vulnerability remediation
- **BigFix Compliance** to continuously monitor and enforce endpoint security configurations and ensure compliance with regulatory or organizational security policies using thousands of out-of-the-box compliance checklists.
- **BigFix Inventory** to discover and manage over 100,000 software titles, reduce software license costs and mitigate security risks of unauthorized software.
- **BigFix Insights** unifies and analyzes data from BigFix and third-party solution providers with deep analytics, new business processes, and powerful reporting.
- **BigFix Mobile** extends modern endpoint management capabilities to iOS and Android devices.

Visit www.hcltechsw.com/bigfix/offerings/products for more information.
.

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, a division of HCL Technologies (HCL) develops, markets, sells, and supports over 30 product families in the areas of Customer Experience, Digital Solutions, DevSecOps, and Security and Automation. HCL Software is the cloud native solution factory for enterprise software and powers millions of apps at more than 20,000 organizations, including over half of the Fortune 1000 and Global 2000 companies. HCL Software's mission is to drive ultimate customer success with its IT investments through relentless product innovation.

072021