HCLSoftware

HCL BigFix Compliance

Maintain continuous compliance according to your needs and enforce them automatically 24/7 with the power of BigFix

HCL BigFix

The number of security threats that compromise endpoints and cause business level damages has been continually growing. With an ever increasing mobile workforce and new cloud initiatives, the very nature of the endpoint is changing. Heightened regulatory concerns put additional burdens on already overtaxed IT teams.

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 protect endpoints and reduce the attack surface with minimal administrative effort.

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. The low impact on endpoint operations enhances productivity and improves the user experience. Enforcing policy compliance reduces cybersecurity risk and increases audit visibility. The built-in AI agent provides speed and efficiency in compliance with automated audit cycles. What used to take days or weeks can now be done in minutes.

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.
- Automatic remediation of configuration drift back to desired states.
- Over 20,000 out-of-the-box compliance checks are continuously updated by BigFix which dramatically reduces the effort to bring all endpoints into compliance.
- Historical trend reports demonstrate configuration, patch and vulnerability compliance over time.
- Speed vulnerability remediation using CyberFOCUS Analytics using the:
  - -Advanced Persistent Threat (APT) Simulator
  - -CISA Known Exploited Vulnerability Exposure Analyzer
  - -Insights for Vulnerability Remediation
  - -Ability to define and manage Protection Level Agreements (PLAs.)

Key Features

Security configuration management

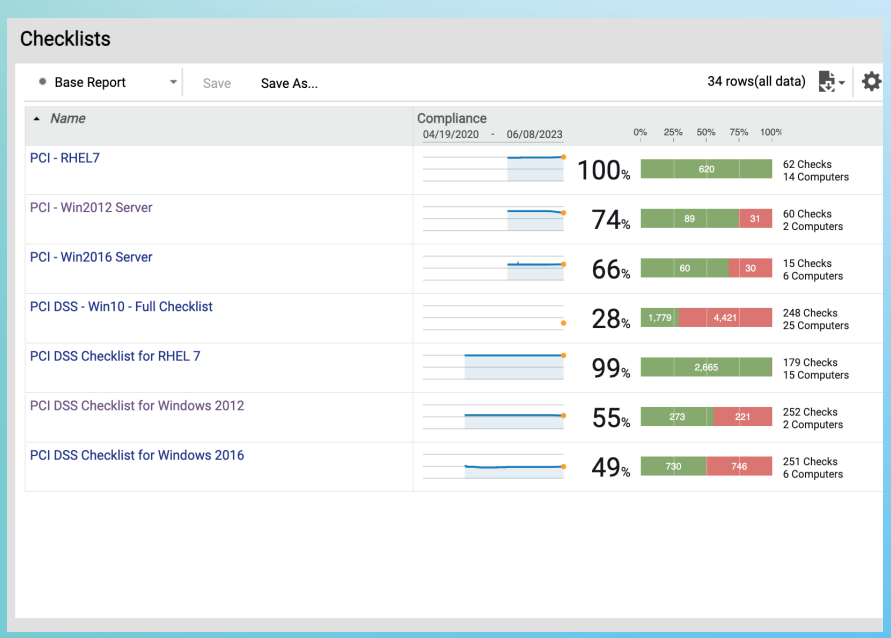
At the core of BigFix Compliance is the ability to maintain **Continuous Compliance** with industry benchmarks using checklists, a set of configuration checks associated with many security benchmarks and guidelines such as the Center for Internet Security (CIS), Defense Information System Agency Security Technical Implementation Guidelines (DISA STIG), Federal Desktop Core Configuration (FDCC), United States Governance Configuration Baseline (USGCB) and Payment Card Industry Data Security Standard (PCI DSS 4.0).

With BigFix Compliance, you can create custom checklists using over 20,000 out-of-the-box checks based on cybersecurity best practices. Additional checks can be easily created to implement unique security policies. Once a checklist is applied to an endpoint, BigFix constantly evaluates the endpoint's security configurations against the deployed checklist. Compliance status is also constantly updated so that configuration drift can be identified and remediated quickly and endpoints are not left vulnerable.

CyberFOCUS Security Analytics

BigFix CyberFOCUS Security Analytics helps organizations discover, prioritize, and patch critical vulnerabilities and reduce cybersecurity risk in real-time, across your global desktop, mobile, datacenter, cloud, and IoT landscape. It includes:

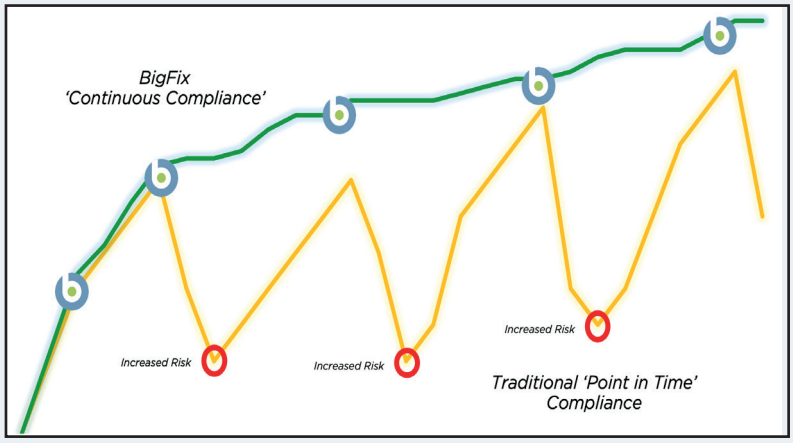
- **Advanced Persistent Threat CVE Analyzer and Vulnerability Remediation Simulator** displays your vulnerabilities grouped by today's more critical Advanced Persistent Threat (APT) families. Here, you can simulate the impact on your attack surface while minimizing downtime caused by patching actions. It also recommends prescriptive remediation actions that maximizes vulnerability attack surface reduction and immediate protection.
- **CISA KEVs Exposure Analyzer** confirms priority exposures to CVEs in CISA's Known Exploited Vulnerabilities Catalog based on available BigFix content. It also



PCI DSS Checklists

What is Continuous Compliance?

BigFix's continuous compliance technology eliminates visibility and compliance gaps by automatically enforcing rules at every endpoint. Continuous compliance will immediately recognize any configuration changes out of compliance on the device and immediately remediate back into compliance.



Traditional point-in-time management solutions "check in" at unpredictable times, reducing viability, creating gaps and increasing risk due to non-compliant endpoints caused by:

- Disconnected endpoints
- Critical patch releases that may take days or weeks to deploy and validate
- Complete patch status reporting that may take days or weeks
- End user-initiated changes affecting security compliance

Because of continuous compliance, BigFix can deliver 99% compliance across the enterprise without operator intervention — slashing compliance costs.

indicates the number of devices exposed, the device vulnerability density, and identifies the biggest attack surface gaps that need to be patched. The Analyzer compares your environment to the CISA-directed due dates for the CVE remediation and indicates your performance against those due dates.

- **Insights for Vulnerability Remediation** integrates with your existing vulnerability assessment tools to be able to prioritize patching at a deeper level and verify that vulnerabilities have been properly remediated with available patch content.
- **Protection Level Agreements (PLAs)** empowers business decisions to be made regarding cyber security risk. It enables business stakeholders and IT/SecOps to balance cyber risks and the cost of protection, and measures patch performance against agreed-to goals.

Compliance analytics

The compliance status of all endpoints against deployed policies are constantly collected, aggregated and reported. The built-in reports show the current status and the historical trends to provide comprehensive analytics for the Security, IT Operations and Compliance teams. With Compliance Analytics, an organization can track the effectiveness of its compliance effort and quickly identify security exposures and risks. Compliance analytics provides the following types of reports:

- **Security configuration reports** shows the current status and historic trend for every endpoint, checklist, and check. An aggregated report on compliance posture shows the overall status and progress of compliance across the entire fleet of endpoints.
- **Patch reports** provide comprehensive and historical view of patching activities and patch compliance across the entire fleet of endpoints. Patch reporting also tracks when each patch is released and applied to each endpoint to help organizations demonstrate compliance and satisfy auditors.
- **Vulnerability reports** focus on tracking and reporting of an endpoint's vulnerability posture as a result of patching actions. This allows organizations to identify risks and demonstrate compliance.

Patch management

Patch management includes comprehensive capabilities for delivering patches for Windows, UNIX, Linux and macOS and for third-party application, database and middleware vendors, including Adobe, Mozilla, Apple, and Oracle.

A single management server can support up to 300,000 endpoints, shortening patch times 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, who deployed them, and confirmation that patches were applied for a complete closed-loop solution to the patching process.

Multivendor endpoint protection management

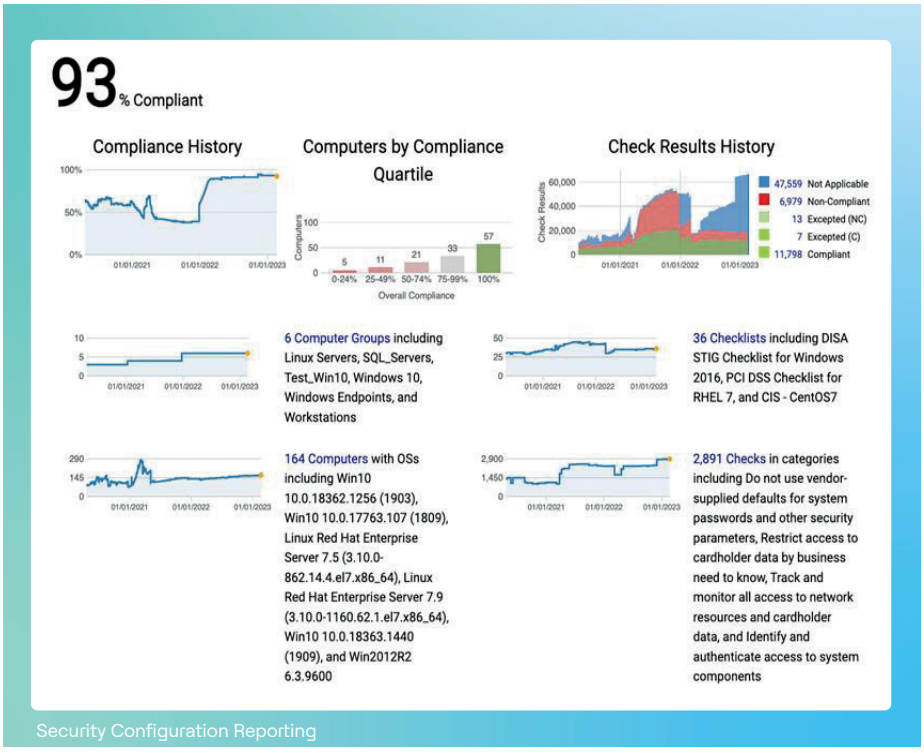
BigFix Client Manager for Endpoint Protection (CEMP) , a component of BigFix Compliance, provides centralized management and control of endpoint protection solutions, ensuring they are always running and kept up to date for reduced cybersecurity risk. It manages third-party antivirus and endpoint protection clients from vendors such as McAfee, Symantec, Trend Micro, Sophos, and Microsoft.

Quarantine of non-compliant systems

Many organizations need to strictly control how endpoints can access the corporate intranet. BigFix Compliance can quarantine endpoints based on their status or configuration against a customized, predefined policy. If an endpoint is discovered to be out of compliance, BigFix Compliance can place the endpoint in network quarantine until it is compliant. A quarantined endpoint can still be managed by BigFix so that it can be remediated, but all other network access is disabled.

Fast endpoint query

BigFix Query provides real-time status of all your endpoints, enabling accurate identification and inspection of vulnerable devices. 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



Security Configuration Reporting

help you identify additional security threats. Users can access 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.

Device discovery

With BigFix Compliance, device discovery is no longer a snapshot counting exercise. Instead, it provides dynamic situational awareness about changing conditions in the infrastructure. The ability to frequently scan the entire network delivers pervasive visibility and control to help ensure that organizations quickly identify all IP-addressable devices. Device discovery helps maintain visibility into all endpoints including end user devices that are roaming beyond the organization's network.

Multiple deployment options

BigFix Compliance can be deployed on-premise, in your organization's cloud, or on the HCL Cloud. There are two options for utilizing the HCL Cloud: BigFix Compliance on Cloud and BigFix One on Cloud. BigFix Compliance on Cloud delivers only the capabilities of BigFix Compliance while BigFix One on Cloud delivers all the capabilities of BigFix Lifecycle, BigFix Inventory, and BigFix Compliance in a single cloud solution.

Prerequisites

- BigFix Compliance on the BigFix Platform 10.0.8 or later
- Microsoft Windows Server 2012, 2012 R2, 2016, or 2019
- Microsoft SQL Server 2012, 2014, 2016, or 2019
- A supported browser

About HCLSoftware

HCLSoftware develops, markets, sells, and supports product families in the areas of Digital Transformation, Data, Analytics & Insights, AI & Automation and Enterprise Security platforms. HCLSoftware is the cloud-native solution factory for enterprise software and powers millions of apps at more than 20,000 organizations, including more than half of the Fortune 1000 and Global 2000 companies. HCLSoftware's mission is to drive ultimate customer success with its IT investments through relentless product innovation.