HCL SOFTWARE | BIGFIX

HCL

Implementing CIS Controls with **BigFix**

www.bigfix.com

As the threat landscape continues to expand and breaches continue to grow in size and scale, organizations are strongly encouraged to implement prioritized security controls to protect the organizations and data from various cyber attacks. Developed by many leading security experts based on threat data and security incidents across the industries, the CIS Controls consists of a set of recommended security best practices to be implemented by all organizations to block security attacks and establish a better defense posture.

HCL BigFix is an effective endpoint management solution to help organizations discover, manage and protect all their endpoints. This document explains how organizations can use BigFix in their efforts to implement many of the CIS Controls.

More information about the recommended CIS controls, visit **https://www.cisecurity.org/controls/cis-controls-list/.**

How BigFix can help

Control 1 | Inventory and control of hardware assets.
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

- BigFix asset discovery can discover all computing assets with an IP address on a network through distributed NMAP scanning. Default reporting lists all the endpoints on a network that are not managed with BigFix, making it easy to detect unauthorized devices.
- BigFix can also be integrated with a Network Access Control (NAC) solution that can check a device's status (e.g. whether the device has a BigFix Agent installed or whether the device complies with a specific security policy) to authorize the device's network access.

Control 2 | Inventory and control of software assets.

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

- BigFix Inventory provides a centralized software asset inventory with detailed information on all installed software applications across all devices. It provides deep insights into what the organization owns—and what it has installed but does not own—along with how often the software is being used, enabling comprehensive software asset inventory for license reconciliation or compliance purposes.

- BigFix inventory can also detect and report the software installed by users but not authorized by the organization, to help enforce the organization's software asset policies.

Control 3 | Continuous vulnerability management.

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

- BigFix Compliance consists of agent-based vulnerability scanning for windows systems, based on the standardized Open Vulnerability and Assessment Language (OVAL) security vulnerability definitions published by CIS, to provide continuous vulnerability assessment.

- As part of the BigFix 10 release, BigFix Compliance will also include a new vulnerability reporting module to evaluate and report, on a daily basis, the vulnerability posture and historical trend of each monitored system, based on the system's current patch deployment status. Reported vulnerabilities are linked to the available patches to help IT Operation prioritize the remediation effort.

Control 4 | Controlled use of administrative privileges.

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

- BigFix Compliance provides a broad set of OS platform and middleware application checklists to help organizations establish a secure configuration environment and enforce specific security policies. Some of the checks are used to restrict the privileges of administrative accounts such as creation of additional accounts, logon policy, password policy, use of specific ports, protocols, devices, and services.

Control 5: Secure configuration for hardware and software on mobile devices, laptops, workstations and servers.

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

- BigFix Compliance centrally manages configuration settings of systems for organizations with large, complex, distributed and heterogeneous computing infrastructures. BigFix Compliance provides platform and application specific configuration checklists out-of-the-box that are developed based on CIS and DISA STIG benchmarks and are easily customizable to support specific regulatory requirements or organization policies. In summary, BigFix Compliance can help organizations:
  - Establish security configuration baselines that meet the regulatory or organization polices.
  - Continuously assess the compliance status on each system against the desired policy and report the compliance posture on individual systems or across the entire environment.
  - Monitor configuration drift and remediate the configuration setting back to the desired state.

Control 6 | Maintenance, Monitoring, and Analysis of Audit Logs.

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

- While BigFix is not a log management or SIEM solution, BigFix can be configured to report on changes on managed systems for monitored compliance policies, patch status and other properties that may be related with a security event.
- BigFix Compliance provides security configuration checks to help ensure all system events or administrative activities are logged.

Control 7: Email and Web Browser Protections.

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

- BigFix Compliance has checklists to help organizations secure the configurations of popular web browsers such as Microsoft IE, Google Chrome.
- BigFix Inventory can monitor and track the brands and versions of email and web browser software installed on devices, to help ensure all software versions are up-to-date.
- Google Chrome is one of the 17 windows applications supported by BigFix Patch, so organizations can use BigFix Patch to keep the browser always patched and protected from vulnerability exploitation.

Control 8: Malware Defenses.

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

- BigFix Compliance contains a Client Manager for Endpoint Protection (CMEP) module that provides real-time visibility and a single point of control for third-party anti-virus or anti-malware solutions from various vendors including Symantec, McAfee, Trend Micro, Sophos, and Microsoft. The Compliance CMEP module monitors and reports if an anti-virus client on each managed system is running correctly or whether its virus definition is outdated. It also provides remediations to address these out-of-policy issues.

Control 9: Limitation and Control of Network Ports, Protocols and Services.

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

- BigFix Compliance has checklists to help organizations limit and control the use of network ports, protocols and services on all managed systems. There are checks available to ensure that a host-based firewall or other security tools are running to protect the system from network attacks. Any policy deviation will be detected and reported immediately so remediations can be taken quickly.

- BigFix Compliance provides a capability to 'quarantine' a system so the system's network access can be disabled, while maintaining a connection with the BigFix Server. This quarantine capability is effective in isolating a system from the network when it is not compliant with a security policy, to mitigate the risks associated with any vulnerability exploited by malware.

Control 10: Data Recovery Capability.

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

- In the event of a system crash, BigFix Lifecycle provides capabilities for OS deployment (bare metal image) and software distribution, to help organization saves efforts and time in recovering business-critical systems.

Control 11: Secure configuration for network devices, such as firewalls, routers and switches.

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

- While BigFix does not manage network devices directly, BigFix Compliance can secure the configurations of computing systems that are used to control and manage the network devices.

Control 12: Boundary Defense.

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

- Not applicable, as a network-based IPS, installed at the network boundary, is the main solution recommended for this control.

Control 13: Data Protection.

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

- While BigFix is not a data protection focused solution, BigFix Compliance contains capabilities and checklists to help organizations ensure security measures that can reduce the likelihood of data exfiltration, such as hard drive encryption, host-based firewall, use of specific ports and services, and file system access control, are deployed on all systems.

Control 14: Controlled Access Based on the Need to Know.

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

- Recommended solutions for this control include VLAN, Encryption, DLP, etc. BigFix supports user-based or role-based access control so administrative staff can be granted privileges to administrate separate systems or assets, or perform different management tasks, enabling organizations to implement controlled access based on their need to know.

Control 15: Wireless Access Control.

The processes and tools used to track/control/prevent/correct the security use of Wireless Local Area Networks (WLANs), access points, and wireless client systems.

- BigFix Compliance can assess and remediate security configurations associated with wireless access on managed systems.

- BigFix can also be integrated with a Network Access Control (NAC) solution that can check a device's status (e.g., whether the device has a BigFix Agent installed or whether the device complies with a specific security policy) to authorize the device's network access.

Control 16: Account Monitoring and Control.

Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

- BigFix Compliance checklists restrict the creation of admin or system accounts, logon policies such as two-factor authentication, and password policies such as password length and password expiration on managed systems.

Control 17: Implement a Security Awareness and Training Program.

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

- This is internal to each organization.

Control 18: Application Software Security.

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

- BigFix Inventory provides a centralized software asset inventory with detailed information on all installed software applications across all devices. For each application supported, it reports the publisher, version, patch level, end of support date, etc., so an organization can have a comprehensive understanding of its installed applications software
- **Note:** HCL AppScan is a solution for scanning internally developed applications for vulnerabilities, as required by this control.

Control 19: Incident Response and Management.

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

- This is internal to each organization.

Control 20: Penetration Tests and Red Team Exercises.

Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

- This is internal to each organization. Penetration testing is a solution for this control.

Summary

CIS Controls offer a way to signifcantly improve the security posture of most organizations. This paper outlines how HCL BigFix can address many of the CIS requirements to improve security posture, reduce the attack surface, and improve consistent compliance.

BigFix is the only endpoint management platform that enables IT/Security Operations to fully automate discovery, management and remediation of endpoints on-prem or in the cloud, regardless of location or connectivity. Unlike complex tools that cover a limited portion of endpoints and takes days or weeks to remediate, BigFix can find and fix all endpoints faster than any other solution.

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 o erings 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.