HCLSoftware

BigFix Support of NIST 800-53 Security Controls

NIST 800-53, published by National Institute of Standards and Technology, is a catalog of Security Controls recommended for all U.S. federal information systems and organizations. NIST 800-53 Revision 5 contains 20 Control Families with each Control Family consisting of a set of related Security Controls. BigFix, an industry leading endpoint management and security solution, has been used by customers to comply with NIST 800-53. This document describes how the various Security Controls in each Control Family are supported by BigFix.

HCL BigFix

HCLSoftware

Table of Contents

Control Family: Access Control

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=AC

Security Control	Support by BigFix
AC-3: Access Enforcement	BigFix provides user based or role based access control so different operators can be granted privileges to administrate different endpoints or content sites, or perform different management tasks.
AC-5: Separation of Duties	BigFix can grant different Operators privileges to manage different groups of endpoints or different BigFix content sites to help meet a separation of duties policy required by an organization.
AC-6: Least Privilege	BigFix Operators by default when they are created are granted no privileges over any information system. Administrative rights must be explicitly assigned by a Master Operator to perform management tasks.
AC-7: Unsuccessful Login Attempts	BigFix Compliance can enforce policies per DISA STIG, USGCB, or CIS checklists to restrict access to an information system by forcing authentication through Windows Domain/Active Directory or other integrated central AAA system which manages and enforces a logon policy so a user may be locked out after a specific number of failed logon attempts.
AC-8: System Use Notification	BigFix Compliance supports assessment and remediation of misconfigured system user notification banners. The banner messages assessed are customizable to support the specific needs of different information system owners.
AC-10: Concurrent Session Control	BigFix Compliance can assess and remediate security configuration controls for restricting the maximum number of concurrent sessions of each account, in support of DISA STIG, USGCB, or CIS benchmarks.
AC-11: Device Lock	BigFix Compliance can assess and remediate security configuration controls for the conditions when a user's local session should be locked after a time period of inactivity, in support of DISA STIG, USGCB, or CIS benchmarks.
AC-12: Session Termination	BigFix Compliance can assess and remediate security configuration controls for the conditions when a user's local session should be terminated, in support of DISA STIG, USGCB, or CIS benchmarks.
AC-17: Remote Access	BigFix Compliance can assess and remediate security configuration controls for remote access to specific information system in support of DISA STIG, USGCB, or CIS benchmarks. BigFix Lifecycle also provides Remote Control capabilities to allow an administrator to remotely access and control an endpoint, in a peer to peer mode.
AC-18: Wireless Access	BigFix Compliance can assess and remediate security configuration controls for wireless access to information systems in support of DISA STIG, USGCB, or CIS benchmarks. BigFix also provides general device management capabilities enabling the establishment of policies on individual computer use of wireless network adapters, including dynamic policies based on computing device location and other variables.
AC-20: Use of External Information Systems	BigFix 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. An external information system can still be managed by BigFix as long as a BigFix Agent is installed on the system. 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 Family: Auditing and Accountability

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=AU

Security Control	Support by BigFix
AU-2: Auditable Events	BigFix can be configured to report on changes on managed systems for monitored compliance policies, patch status and other properties. BigFix can also be used to filter and report on system or security events from Operating System event or audit logs.
AU-6: Audit Review, Analysis, and Reporting	BigFix is able to produce reports and snapshots of system configurations, patch status, computer properties and other monitored issues. The reports can be generated on a scheduled basis or in conjunction with customizable triggers to assist in auditing the status of information systems.
AU-12: Audit Generation	BigFix can be configured to report on changes on managed systems for monitored compliance policies, patch status and other properties. BigFix can be used to filter and report on system or security events from Operating System event or audit logs.

Control Family: Awareness and Training

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=AT

No specific Security Control in this Control Family applies to BigFix.

Control Family: Configuration Management

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=CM

Security Control	Support by BigFix
CM-1: Policies and Procedures	BigFix Compliance provides capabilities to create and enforce security configuration policies that are implemented or customized based on DISA STIG, USGCB, or CIS benchmarks. These system level, technical policies can be used to support an organization's configuration management policies defined at the organization level.
CM-2: Baseline Configuration	BigFix Compliance supports the development of security configuration baselines and assess and report compliance against those baselines over time. It also supports continuous policy enforcement to eliminate configuration drift quickly. BigFix Patch and Lifecycle provide capabilities to maintain a consistent software and patch baseline across all endpoints. BigFix Inventory provides capabilities to report installed software packages installed on all endpoints. All these capabilities can help an organization establish and maintain baseline configurations across the information systems.
CM-3: Configuration Change Control	BigFix Compliance supports configuration change control through the control of specific remediation to systems by BigFix Operators with appropriate authority. The type of configuration change control actions that may be performed can be tailored to the operators. For example, one operator may have authority to define and publish change control contents, while another operator may only have rights to implement the defined change contents on specific endpoints.

CM-4: Impact Analysis	BigFix provides capabilities to easily establish a test group of computers within the application and apply desired changes and remediation to only those systems in the test group, in order to validate the impact of the change prior to implementing the change on all production systems. BigFix also provides various reports to show the impact of the changes on the systems (e.g., if a compliance posture has been enhanced after remediation) so an organization can verify that the implemented changes are producing the desired outcome.
CM-5: Access Restrictions for Change	BigFix restricts the configuration changes to individual systems by assigning access rights for specific systems or performing specific tasks to individual operators or roles.
CM-6: Configuration 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 that are based on DISA STIG, USGCB, or CIS and are customizable to support specific regulatory requirements or organization policies. BigFix provides functionalities to help organizations: • Establish security configuration baselines to meet the regulatory or organization polices • Assess the compliance on each system against the baseline and report the compliance posture on individual system or across the entire infrastructure • Monitor the configuration drift and remediate the configuration setting back to the proper state
CM-7: Least Functionality	BigFix Compliance provides platform and application specific checklists to enforce specific configurations, including restricting the use of specific ports, protocols, devices, services, etc. Custom fixlets can also be created to restrict the use of a specific function on a system.
CM-8: System Component Inventory	BigFix Inventory provides a centralized information system inventory with detailed information on hardware specifications, installed software applications and version, license usage, etc. It can even be used to scan the entire file system to report all the files, their hash values, and other properties on a system.
CM-10: Software Usage Restrictions	BigFix Inventory centrally monitors the installed software applications and tracks the license usage on each system, based on vendor/application specific licensing metrics, to help organizations comply with their authorized license quantities.
CM-11: User-Installed Software	BigFix Inventory can be used to detect and report the software installed by users, to help organizations enforce the policies governing the user-installed software.

Control Family: Identification and Authentication

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=IA

Security Control	Support by BigFix
IA-5: Authenticator Management	BigFix Compliance provides platform or application specific checklists, in support of DISA STIG, USGCB, or CIS, to help enforce password (authenticator) related policies such as minimum password length, password reuse number, the maximum number of failed logon attempts.

Control Family: Contingency Planning

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=CP

Security Control	Support by BigFix
CP-10: System Recovery and Reconstitution	BigFix Lifecycle provides capabilities for OS deployment (bare metal image) an software distribution, which can help organization saves effort and time for recovering business critical systems.

Control Family: Incident Response

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=IR

Security Control	Support by BigFix
IR-4: Incident Handling	BigFix has an agent running on each managed system that can be instructed to monitor and detect any system event or change that contributes to the occurrence of a security incident. The detected event can then be used to trigger additional incident handling activities. BigFix is integrated with IBM Resilient to provide additional artifacts for specific systems to help a Resilient user investigate and analyze a security incident. The integration also allows a Resilient user to take immediate remediation action (killing a process, removing a file, etc.) on a system.

Control Family: Maintenance

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=MA

Security Control	Support by BigFix
MA-2: Controlled Maintenance	BigFix provides patch management, software distribution and inventory, and security configuration management that can all be used as maintenance tools to help organizations effectively perform scheduled maintenance on information systems. All changes to the systems are logged and can be used as part of the maintenance records.
MA-4: Nonlocal Maintenance	BigFix performs all management tasks on systems remotely by an agent installed and running on each system. A BigFix Operator needs to log on to BigFix Console and can only perform the management tasks allowed by the granted access rights. All tasks performed on local systems are centrally stored and maintained.
MA-6: Timely Maintenance	BigFix management tasks can be scheduled to occur at a specific time points, to support the system maintenance widows specified in an organization's maintenance policy/program.

Control Family: Media Protection

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=MP

No specific Security Control in this Control Family applies to BigFix.

Control Family: Personnel Security

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=PS

Security Control	Support by BigFix
PS-4: Personnel Termination	BigFix can be leveraged to reduce the risk associated with computing devices not returned after an employee is separated from the organization. For example, the devices can be quarantined so it won't have any access to network (except with BigFix Server) or customer fixlets can be created to remotely remove business applications and data on devices.
PS-5: Personnel Transfer	BigFix Compliance can be leveraged to enforce new security configuration policies on the devices when an employee is transferred to another organizational group where a new security policy is required based on the mission of the new group or the employee's new role.

Control Family: Personally Identifiable Information Processing and Transparency

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=PT

No specific Security Control in this Control Family applies to BigFix.

Control Family: Physical and Environment Protection

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=PE

No specific Security Control in this Control Family applies to BigFix.

Control Family: Planning

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=PL

Security Control	
PL-2: System Security and Privacy Plans	BigFix provides many functions that can play important roles in implementing an organization's security plan, such as security configuration assessment, hardware/software inventory, patching management, etc. All the BigFix management tasks that affect the information systems' states can be planned and scheduled to happen at specific time point so the impact to the organization can be minimized.
PL-9: Central Management	BigFix controls and manages all the BigFix components and artifacts (agent, sites, policies, fixlets, baselines, etc.) in BigFix Console or WebUI'. All the monitoring or execution results collected from each BigFix agent are stored in a centralized database and reported on a single UI.

Control Family: Program Management

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=PM

Security Control	Support by BigFix
PM-5: System Inventory	BigFix Inventory provides a centralized information system inventory with detailed information on hardware specifications, installed software applications and version, license usage, etc. It can even be used to scan the entire file system to report all the files, their hash values, and other properties on a system.
PM-6: Measures of Performance	BigFix Compliance monitors and assesses the security configurations of all information systems against pre-defined policies and reports the policy compliance results, in different measures, such as an overall compliance score, a breakdown of all systems in each quartile of compliance, and a historical trend of compliance progress.
PM-10: Authorization Process	BigFix provides user based or role based access control so only authorized operators can be granted privileges to administrate different groups of endpoints or content sites, or perform different management tasks.

Control Family: Risk Assessment

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=RA

Security Control	Support by BigFix
RA-2: Security Categorization	BigFix provides capabilities to group all managed information systems to different groups, as a way to support the security categories defined based on an organization risk assessment program. Different security policies can then be applied to different groups.
RA-3: Risk Assessment	BigFix Compliance provides capabilities to support all the various steps conducted in risk assessment, including: • Security Categorization: by grouping all endpoints to different groups • Security Control Selection: by determining what specific security checks to adopt and customize if necessary • Security Control Implementation: by applying the security checklists to specific endpoints or groups. • Security Control Assessment: by continuously assessing the security postures on all endpoints • Information System Authorization: by assigning individual operators appropriate privileges to manage policies or different groups of endpoints • Security Control Monitoring: by continuously collecting the assessment results and reporting the policy compliance state and history
RA-5: Vulnerability Scanning	BigFix Compliance provides agent based vulnerability scanning for Windows systems, based on the standardized Open Vulnerability and Assessment Language (OVAL) security vulnerability definitions published by National Vulnerability Database (NVD). The BigFix vulnerability scanning data is intended to be incorporated and correlated with the vulnerability data scanned from other enterprise-level, cross-platform vulnerability scanners. BigFix Insights for Vulnerability Remediation integrates BigFix with Tenable and Qualys vulnerability management sources of vulnerability data to guide BigFix users on how to apply the best patch and configuration settings to remediate discovered vulnerabilities, and thus reduce risk and improve security. BigFix Insights for Vulnerability Remediation uses advanced correlation algorithms to aggregate and process the vulnerability data with information from BigFix to drive analytics and reports. It facilitates remediation through the Baseline Creation Wizard by recommending the latest available patches for the discovered vulnerabilities.

Control Family: System and Services Acquisition

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=SA

No specific Security Control in this Control Family applies to BigFix.

Control Family: Systems and Communications Protection

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=SC

Security Control	Support by BigFix
SC-10: Network Disconnect	BigFix Compliance provides a capability to 'quarantine' a system so the system's network access can be disabled except keeping 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 or has not been applied a critical security patch, to help mitigate the risks associated with system vulnerability exploitation by malware.

Control Family: Assessment, Authorization and Monitoring

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=CA

Security Control	Support by BigFix
CA-2: Security Assessments	BigFix Compliance provides security configuration control checks created based on the benchmarks published by DISA STIG, USGCB, CIS, and PCI DSS. The platform specific checklist and individual checks can be customized to support an organization's security assessment needs. Security configurations on all managed systems are continuously assessed and assessment results are centrally reported on a Web based UI. Individual systems that fail the compliance checking can be effectively remediated remotely. BigFix can restrict access to assessment data to specific individuals or groups through RBAC to support separation of duties and the creation of an independent assessment team.
CA-5: Plan of Action and Milestones	BigFix provides continuous, near real-time monitoring, assessment, reporting, and remediation of security patches, vulnerabilities, configurations on all managed systems across various platforms. It serves as an effective, automated mechanism/tool to help an organization ensure the plan of action and milestones for the information system is accurate, up to date, and readily available.
CA-7: Continuous Monitoring	BigFix agent running on every managed system continuously monitors and assesses the patch levels, vulnerabilities, software inventory and security configurations against a set of policies created based on benchmarks published by authoritative bodies such as DISA STIG, USGCB, CIS, and PCI DSS. The monitoring is performed in a continuous manner so any 'drift' from the desires polices can be detected immediately. All system assessment results are centrally collected, analyzed, and reported on Web-based UI. BigFix also provides on-going updates of patch contents, software inventor directory, and security configuration checks to help an organization perform continuous monitoring on all information systems based on the latest contents and policies.

Control Family: System and Information Integrity

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=SI

Security Control	Support by BigFix
SI-2: Flaw Remediation	BigFix Patch provides out of the box patching content for a number of OS platforms including Windows, Unix, Linux, Mac OS, etc. and many common third party Windows and Mac applications from vendors such as Adobe, Mozilla, Google, Oracle (Java), etc. A patch can be a security patch for remediating specific vulnerabilities or a non-security patch for fixing software flaws. For each patch available, BigFix helps an organization identify the information systems that needs the patch to be applied. An administrator can then apply the patch to the systems effectively with a very high success rate (> 95%) in most cases.
SI-3: Malicious Code Protection	BigFix Compliance contains a module called Client Manager for Endpoint Protection (CMEP), which provides real-time visibility and single point of control for managing various third party malware protection solutions from various vendors including Symantec, McAfee, Trend Micro, Sophos, CA, Microsoft, etc. The CMEP module monitors and reports if an anti-virus client on each managed system is running correctly and whether the virus definition is outdated.
SI-7: Software and Information Integrity	BigFix provides capabilities to monitor and detect the changes to the OS/patch levels, application software assets, and security configurations on managed information systems, to help an organization ensure the integrity of the information system and installed software.
SC-17: Fail-Safe Procedures	BigFix provides mechanisms (agent, fixlets, etc.) to help an organization flexibly implement the steps defined in a fail-safe procedure, such as terminating a service, restarting the system, changing a specific setting, or even re-imaging a system.

Control Family: System and Services Acquisition

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=SA

Security Control	Support by BigFix
SA-10: Developer Configuration Management	BigFix Compliance can be deployed to help ensure the integrity of the machines used by developers of an information system or service, so the configuration states of the machines can be closely monitored, reported, and remediated if integrity compromised, during the entire software development cycle.

Control Family: Supply Chain Risk Management

Reference: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=SR

No specific Security Control in this Control Family applies to BigFix.

Acknowledgment

The content for this whitepaper was provided by I-Lung Kao, HCL Product Manager. I-Lung focuses on BigFix endpoint management and security solutions. With 20+ years of industry experience in various IT security areas, including identity and access management, security intelligence, endpoint compliance, and cloud management, I-Lung has been leading efforts in defining product strategy and delivering cutting-edge solutions to help customers address critical security challenges and realize substantial business values.

For more information about HCL BigFix please visit: www.hclfederal.com

About HCLSoftware
HCLSoftware is a division of HCL Tech (HCL) that operates its primary software business. It develops, markets, sells, and supports over 30 product families in the areas of Digital Transformation, Data Analytics & Insights, AI and Automation, and Enterprise Security. HCLSoftware has offices and labs around the world to serve thousands of customers. Its mission is to drive ultimate customer success with their IT investments through relentless innovation of its products.