

HCLSoftware

Ensuring Public Sector Cybersecurity Resilience: the HCL BigFix Approach

HCL BigFix

Introduction:

In today's rapidly evolving threat landscape, the public sector faces a constant challenge to secure its digital infrastructure against potential cyber threats. The Cybersecurity and Infrastructure Security Agency (CISA) plays a pivotal role in safeguarding national security by providing guidelines and mandates to ensure the resilience of federal systems. One critical aspect of this effort involves addressing known exploitable vulnerabilities (KEV), and HCL BigFix stands out as a comprehensive solution to meet the **compliance requirements set by CISA**.



HCL BigFix's Unique Approach:

HCL BigFix adopts a multifaceted and proactive approach to compliance with CISA's guidelines on known exploitable vulnerabilities, ensuring federal agencies can maintain a robust cybersecurity posture.



Real-time Vulnerability Visibility:

HCL BigFix provides real-time visibility into the vulnerability landscape across the entire federal infrastructure. Through continuous monitoring and scanning, it identifies known exploitable vulnerabilities promptly, allowing agencies to stay ahead of potential threats. This real-time visibility is crucial for meeting CISA's requirements for timely detection and response.



Automated Patching and Remediation:

Automation is at the core of HCL BigFix's solution. Upon identifying known vulnerabilities, the platform automates the patching and remediation process across all endpoints within the federal network. This not only accelerates the mitigation of potential threats but also ensures consistency and accuracy in applying necessary security measures, aligning with CISA's emphasis on proactive vulnerability management.



Comprehensive Compliance Reporting:

HCL BigFix enables federal agencies to generate detailed compliance reports that align with CISA's requirements. These reports provide a comprehensive overview of the vulnerability landscape, actions taken to address known exploitable vulnerabilities, and the overall compliance status. This transparency is essential for federal agencies in demonstrating their adherence to CISA guidelines during audits and assessments.



Customizable Policy Enforcement:

Recognizing the diverse nature of federal IT environments, HCL BigFix allows agencies to tailor vulnerability management policies according to their specific needs. This flexibility ensures that CISA compliance measures are implemented in a manner that best suits each agency's unique infrastructure, taking into account the variety of systems and applications in use.



Continuous Monitoring and Adaptive Security:

HCL BigFix does not limit its capabilities to one-time remediation efforts. Instead, it continuously monitors the federal infrastructure, adapting security measures to emerging threats. This aligns with CISA's emphasis on continuous improvement and proactive security measures to stay ahead of potential vulnerabilities and exploits.



Benefits:

By employing the BigFix approach to CISA KEV, forward thinking agencies have seen many benefits including:



Knowledge of what needs protecting:

Create and maintain an up-to-date inventory of endpoint hardware and software.



Adoption of Unified Endpoint Management

Optimize and streamline IT Operations to help implement consistent security policies across workspace, server and mobile endpoints.



Efficient and effective patching and software updates:

Shorten patch cycles across and unify patching of Windows, UNIX, Linux, macOS and mobile OSs.



Proven cyber risk reduction.

Show executives real-time endpoint compliance levels and prove cyber risk reduction using Protection Level Agreements.



Elimination of configuration drift:

Continuously monitor and enforce security policies and system settings.



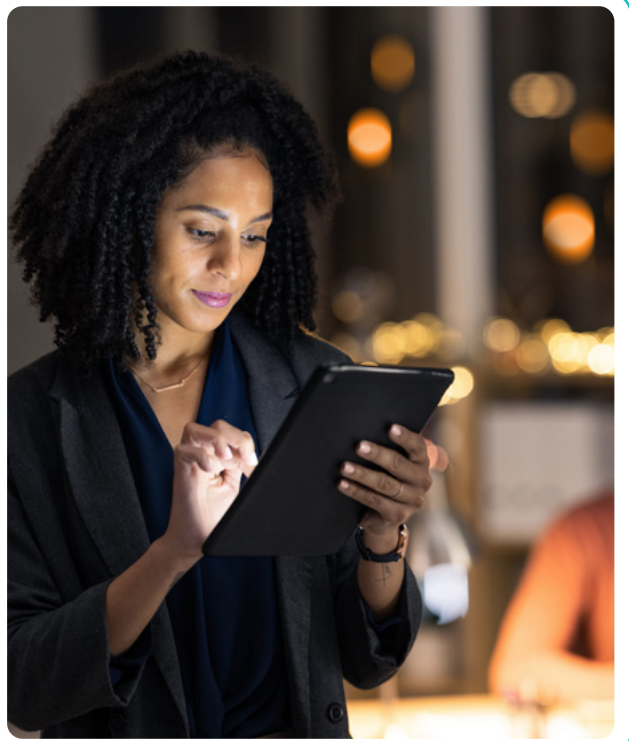
Easy compliance with industry standards:

Utilize out-of-the-box but customizable checklists for compliance with PCI DSS, CIS, DISA STIG, and others.



Remediation of known exploited vulnerabilities fast

Identified, prioritize and remediate exploited vulnerabilities using threat intelligence by CISA and MITRE.



Conclusion:

In the face of evolving cyber threats, federal agencies need a dynamic and comprehensive solution to comply with CISA guidelines on known exploitable vulnerabilities. HCL BigFix stands as a reliable partner, offering a holistic approach that encompasses real-time visibility, automated patching, compliance reporting, customizable policy enforcement, and continuous monitoring. By leveraging HCL BigFix, federal agencies can enhance their cybersecurity resilience, effectively mitigate known vulnerabilities, and demonstrate unwavering commitment to CISA's mandates in safeguarding agency security.

[Learn more](#)



About HCLSoftware

HCLSoftware is a division of HCLTech (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.

HCLSoftware

hcl-software.com