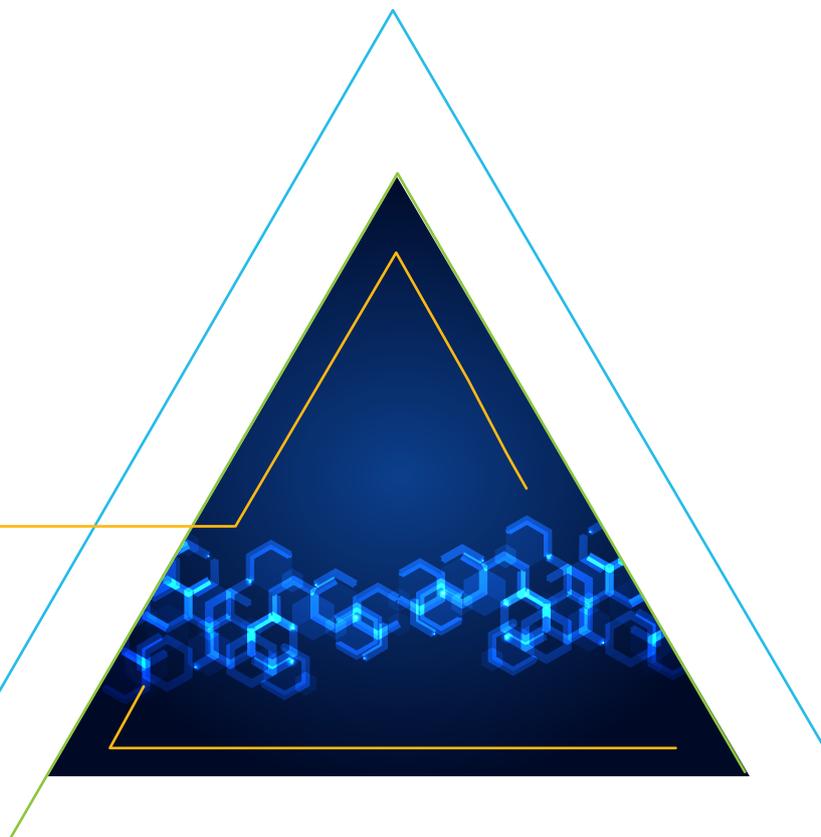# BigFix Insights for Vulnerability Remediation Integration with Tenable

HCL BigFix announces Strategic Partnership with Tenable to align security and IT operations teams and dramatically compress vulnerability resolution time

Today, it can take days or weeks for IT Operations to remediate vulnerabilities found by IT Security, exposing organizations to potential attacks. As a result, mitigating the risk of cyberattacks continues to top CIO and CISO lists of concerns. Companies who detect vulnerabilities using Tenable® are focused on seeking out vulnerabilities across the organization. IT operations teams using BigFix® systemically find and deploy the right patch for each unique vulnerability identified by Tenable. In many cases, there is a communication gap between the two organizations, resulting in excessive manual effort, spreadsheet errors and long windows of vulnerability. In fact, studies show that up to one-third of all detected vulnerabilities remain open after a year, and over one-quarter are never remediated.

BigFix Insights for Vulnerability Remediation can reduce the time it takes for IT Operations to remediate vulnerabilities found by IT Security from days or weeks to minutes or hours. BigFix Insights for Vulnerability Remediation automatically correlates vulnerabilities discovered by Tenable with the most appropriate patch and configuration settings enabling organizations to quickly prioritize remediation actions, reducing the enterprise attack surface. Unlike other solutions. BigFix leverages the broadest set of remediation capabilities, both in terms of supported OS platforms, and out of-the-box, certified remediations.

The BigFix Insights for Vulnerability Remediation application is designed specifically for organizations who use BigFix Lifecycle and BigFix Compliance and who also use Tenable for vulnerability management.
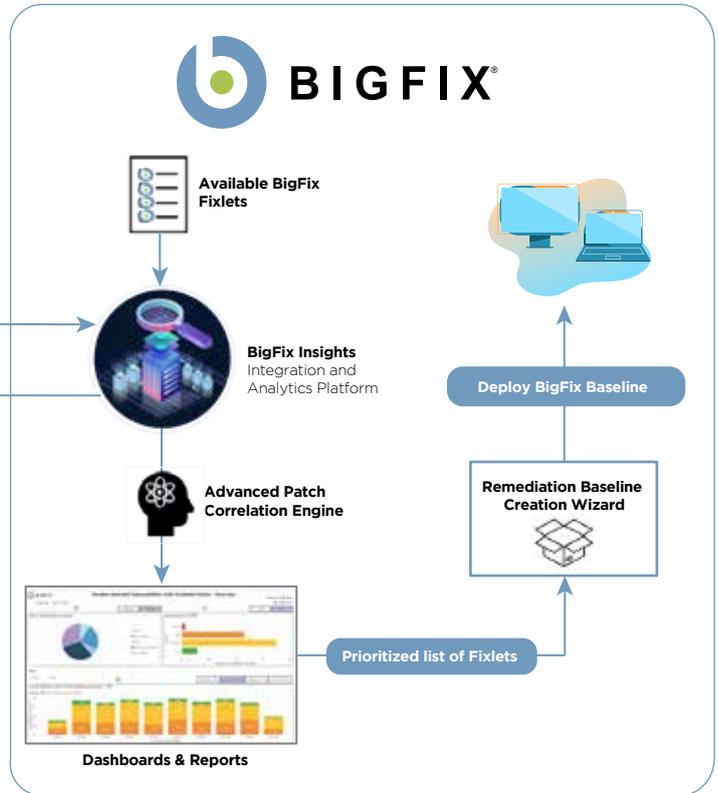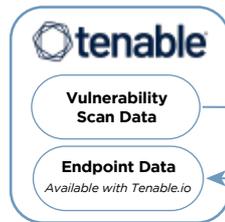
Highlights

- Dramatically reduce the gap between Security and IT operations, improving awareness of what remediation steps are needed to close discovered vulnerabilities

- Automatically correlates Tenable's Vulnerability Priority Rating (VPR) prioritized vulnerabilities with the recommended remediation Fixlets using four separate correlation engines, while providing the data you need to effectively prioritize remediation actions

- Tenable.io users with Tenable Lumin can better understand organizational risks to better prioritize which vulnerabilities on which endpoints should be remediated first by using Tenable's ACR (Asset Criticality Rating) and AES (Asset Exposure Score)

Speed Remediation of Vulnerabilities - How it works

BigFix Insights for Vulnerability Remediation speeds remediation by automating manual processes that are commonly seen in organizations. Automated correlation of vulnerability scan data from Tenable with available Fixlets from BigFix speeds remediation of endpoint vulnerabilities across the enterprise.

The operational flow is:

1. A Security Operator performs a scan using Tenable to identify the vulnerabilities across the enterprise.

2. The vulnerabilities or Common Vulnerabilities and Exposures (CVE®) identified by Tenable are automatically imported into BigFix Insights and combined with BigFix's comprehensive patch data.

3. BigFix Insights for Vulnerability Remediation then uses our Advanced Patch Correlation engine to vulnerability scan data with vulnerability scan data with the latest BigFix patches.

4. BigFix users can review several easy-to-read dashboards and reports to identify actionable and prioritized vulnerabilities that can be immediately remediated with available BigFix Fixlets.

   A BigFix user in IT Operations can leverage the Remediation Baseline Creation Wizard to automatically create baselines, and then deploy the baseline to the target endpoint, completing the patch cycle.

BigFix Insights for Vulnerability Remediation Operational Flow

Using this operational workflow, organizations using Tenable can leverage BigFix Insights for Vulnerability Remediation to dramatically reduce the remediation time, errors and the attack surface.

BigFix Insights for Vulnerability Remediation - A Case Study

A Fortune 10 financial institution was spending **43 person-hours per month** remediating vulnerabilities found by IT Security. With BigFix Insights for Vulnerability Remediation, this time was reduced **to less than 2 hours** through automation of manual processes and reduction of errors and the associated rework.

For the first time, the financial institution's IT organization was able to effectively prove compliance to auditors and executive stakeholders.

With BigFix Insights for Vulnerability Remediation, the IT Security and IT Operations teams were able to collaborate effectively to quickly remediate vulnerabilities discovered by Tenable. Significant value was delivered to both the CIO and CISO through:

• Aligning Security and Operations teams with intelligent automation

• Compressing security vulnerability remediation times by an order of magnitude

• Reducing enterprise security risk.

Time to Remediate Vulnerability Scan Data
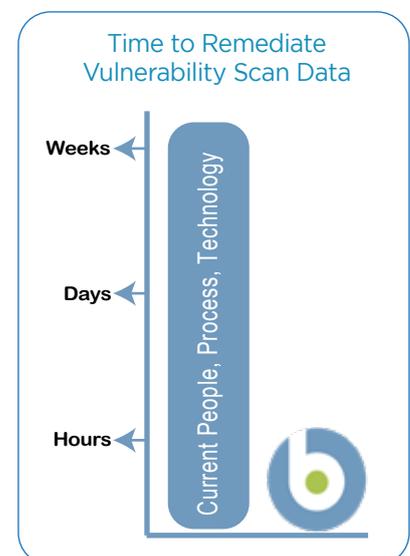
BigFix Vulnerability Correlation Dashboard

The Tenable-Vulnerability Correlation Dashboard provides actionable views of the correlated data from Tenable and BigFix. Each view helps IT and Security operators understand the magnitude and severity of the vulnerabilities in different ways to enable effective prioritization of remediation actions. Operators can leverage the interactive dashboard to drill down to more detail associated with the correlated vulnerabilities and devices.

Four Levels of Granularity

(1) *Graphical overview* - comprises three graphs or charts for a high-level visual overview to enable very quick prioritization across multiple contexts.

(2) *Data view* - depicts vulnerabilities and their correlated Fixlets, along with the number of affected devices in a tabular format.

(3) *Vulnerability view* - depicts which devices have a specific vulnerability, and the recommended Fixlet for remediation.

(4) *Device view* - shows all the vulnerabilities and the recommended Fixlets for remediation associated with a particular device or endpoint

The graphical view contains the three charts shown below. Each chart leverages Tenable's Vulnerability Priority Rating (VPR) – which goes beyond measuring the technical impact of a vulnerability to also include threat intelligence contexts - to enable prioritization from different perspectives. Some of the charts also offer the ability to view data by CVSS(Common Vulnerability Scoring System) which is an industry standard for assessing the severity of security vulnerabilities.
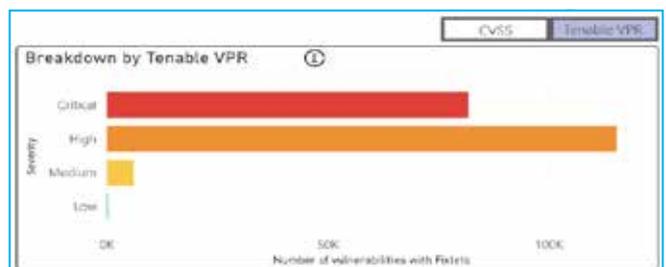
Top 5 Vulnerable Devices

The first chart depicts the top five devices that have the highest sum of VPR scores associated with detected vulnerabilities that can be remediated by BigFix.
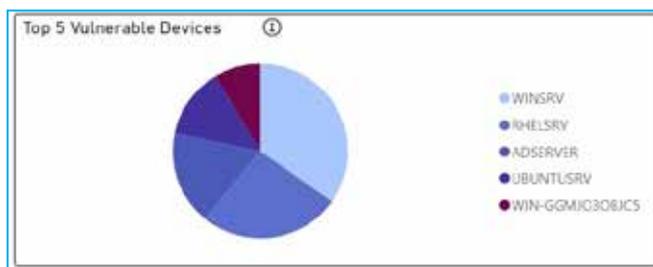
Vulnerabilities by Severity

The second chart depicts vulnerabilities with available Fixlets by Tenable VPR or by CVSS.

Vulnerabilities by Date Detected and Severity

The third chart augments the details provided in the Vulnerabilities by Severity chart. Specifically, this graph adds the date detected and date published. The Date Detected is the date a given vulnerability instance was first detected by Tenable, while the Date Published is the date the vulnerability record was first added to the CVE List. A date range by year can also be specified.

Why BigFix?

The HCL BigFix endpoint management platform gives IT Operations teams the power of Continuous Compliance and Intelligent Automation to manage over 100 operating system versions, enabling streamlined management processes, tool consolidation and reduced operating costs.

Unlike complex tools that cover a limited portion of your endpoints, BigFix's unified architecture can effectively manage and ensure compliance of all your 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 it takes to remediate vulnerabilities by an order of magnitude. 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-premises in a consistent manner.

BigFix's unique approach, coupled with thousands of out-of-the-box security checks, 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-premise, virtual, cloud or mobile– regardless of operating system, location or connectivity. Unlike complex tools that cover a limited portion of endpoints and take days or weeks to remediate vulnerabilities, BigFix can find and fix endpoints faster than any other solution.

The BigFix family includes:

- **BigFix Lifecycle** - Automate endpoint management by enabling software and operating system deployment, continuous compliance, self-service software catalog, power management, server automation, and vulnerability remediation.

- **BigFix Compliance** – Continuously monitor and enforce endpoint security configurations ensuring compliance with regulatory or organizational security policies using out-of-the-box compliance checklists.

- **BigFix Inventory** – Discover and manage over 100,000 software titles to reduce software license costs and mitigate security risks of unauthorized software.

- **BigFix Insights** – Unify and analyze data from BigFix and third-party solutions to enable deep analytics, new business processes, and powerful reporting.

- **BigFix Mobile** – Extend modern endpoint management techniques 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 is a division of HCL Technologies that develops and delivers a next-generation portfolio of enterprise-grade software-based offerings 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.

062021