HCLSoftware

HCL BigFix Insights for Vulnerability Remediation Integration with Tenable

Align security teams using Tenable® with IT operations teams using BigFix and dramatically compress vulnerability resolution time.

HCL BigFix

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.

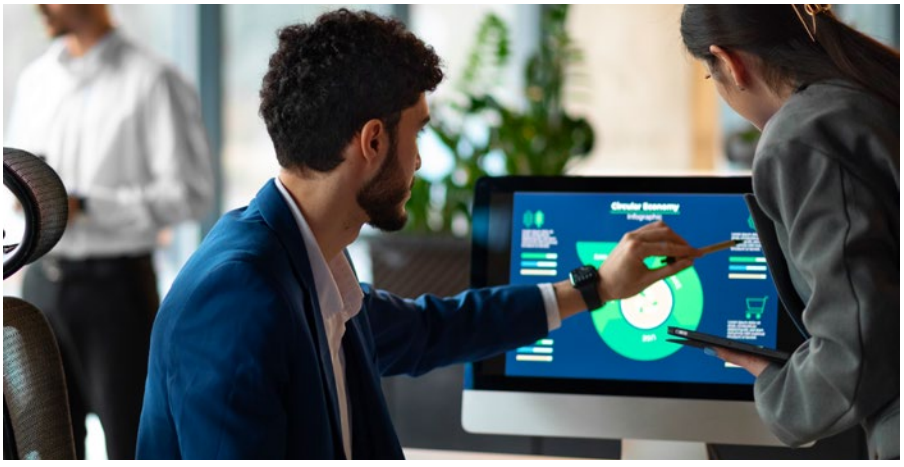
Companies who detect vulnerabilities using Tenable® are focused on seeking out vulnerabilities across the organization. IT operations teams using BigFix® systematically find and deploy the right patch for each unique vulnerability identified by Tenable. In many cases, there is a communication gap between these two teams, 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 and deploy 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.

BigFix Insights for Vulnerability Remediation is designed specifically for organizations who use BigFix Lifecycle, BigFix Compliance, or BigFix Remediate and who also use Tenable for vulnerability management.

Highlights

- Dramatically reduce the gap between Security and IT operations, reducing time required to close discovered vulnerabilities
- Automatically correlates vulnerabilities discovered by Tenable with the recommended remediation Fixlets using BigFix supersedence engine
- Shrinks attack surfaces and closes the loop between vulnerability detection and remediation
- Requires no additional agents or relays and has no impact on the endpoint or network performance



BigFix Remediate can resolve vulnerabilities faster... up to 96% faster!

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. along with simple, prioritized deployment workflows 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

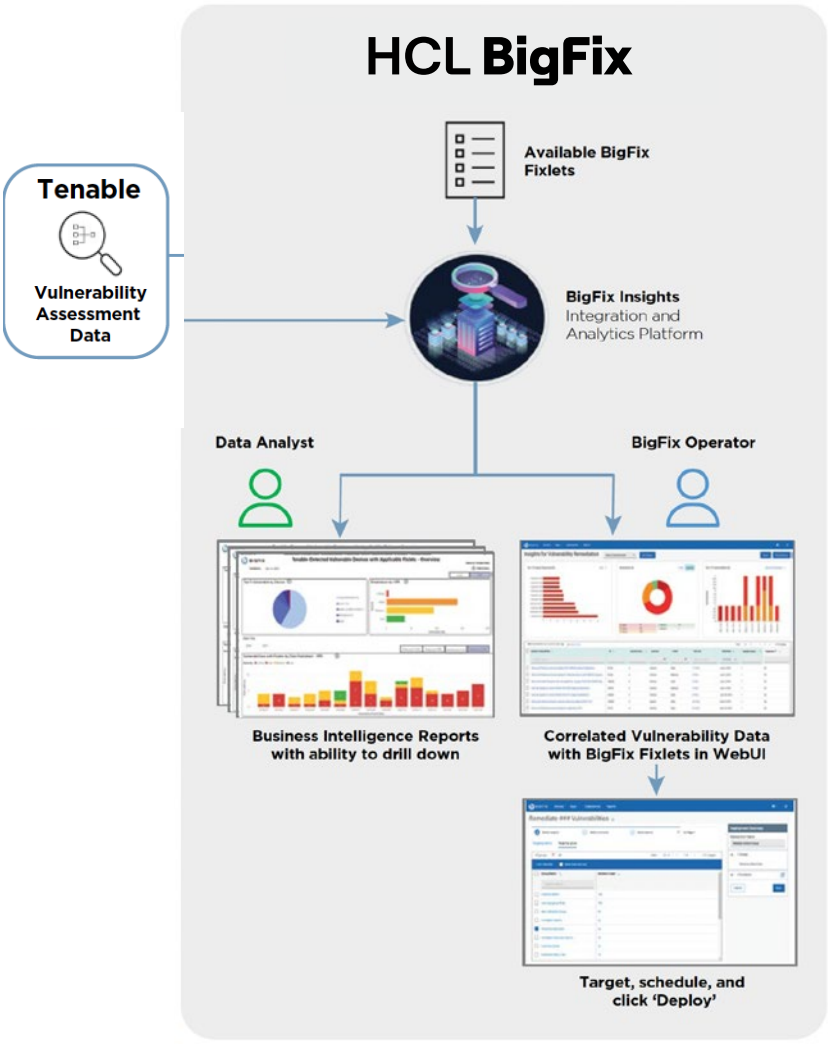
2. The vulnerabilities or Common Vulnerabilities and Exposures (CVE®) identified by Tenable are automatically correlated with BigFix's comprehensive patch data. The process involves:

   a) Correlating the asset for a given vulnerability between Tenable and BigFix
   b) Correlating the vulnerability to a remediation Fixlet
   c) Identifying the latest available (i.e. superseding) remediation
   d) Ensure the given asset still requires the latest available remediation (i.e. Fixlet applicability relevance)

3. After correlation, staff can examine the information and take action.

   a) Data or Security Analysts leverages Business Intelligence Reports, drilling down into the details to better understand the vulnerabilities and potential remediations.
   b) BigFix Operators can leverage the Vulnerability Remediation Dashboard to see vulnerabilities that can be remediated using available BigFix Fixlets, and more importantly, immediately target and deploy remediations.

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



A Case Study of BigFix for Insights Vulnerability Remediation

Typically, an IT operations or Security specialist will spend 2-3 minutes researching the right remediation for each vulnerability. With potentially hundreds or thousands, that is a lot of time spent. BigFix Insights for Vulnerability Remediation automates this process with the Advanced Patch Correlation Engine which:

What does this mean in business terms?

An organization with 1,000 running vulnerabilities will spend up to 50 person-hours per assessment cycle researching and correlating available fixes to the correct assets. With BigFix Insights for Vulnerability Remediation, this time can be reduced to less than two hours by automating manual processes and reducing errors and associated rework. **That is 96% less effort!**

IT organization can also quickly implement fixes and effectively prove compliance to auditors and executive stakeholders. With BigFix Insights for Vulnerability Remediation, IT Security and IT Operation teams can collaborate effectively to quickly remediate vulnerabilities discovered in a prioritized manner, providing significant operational and organizational value to the CIO and CISO.

BigFix Insights for Vulnerability Remediation delivers signification business value by:

- Aligning Security and Operations teams with intelligent automation
- Compressing security vulnerability remediation times by an order of magnitude
- Implementing fixes and proving compliance to all stakeholders
- Reducing enterprise security risk, helping prevent cyberattacks

BigFix Insights for Vulnerability Remediation Application

The BigFix Insights for Vulnerability Remediation Application for Tenable 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 visualizations to filter and to drill down to more detail associated with the correlated vulnerabilities and devices.

Three Granular Views

(1) Graphical overview/summary – Comprises three graphs or charts for a high-level visual overview to enable very quick prioritization across multiple contexts. The three graphs are shown in the top half of the image below and depicts:

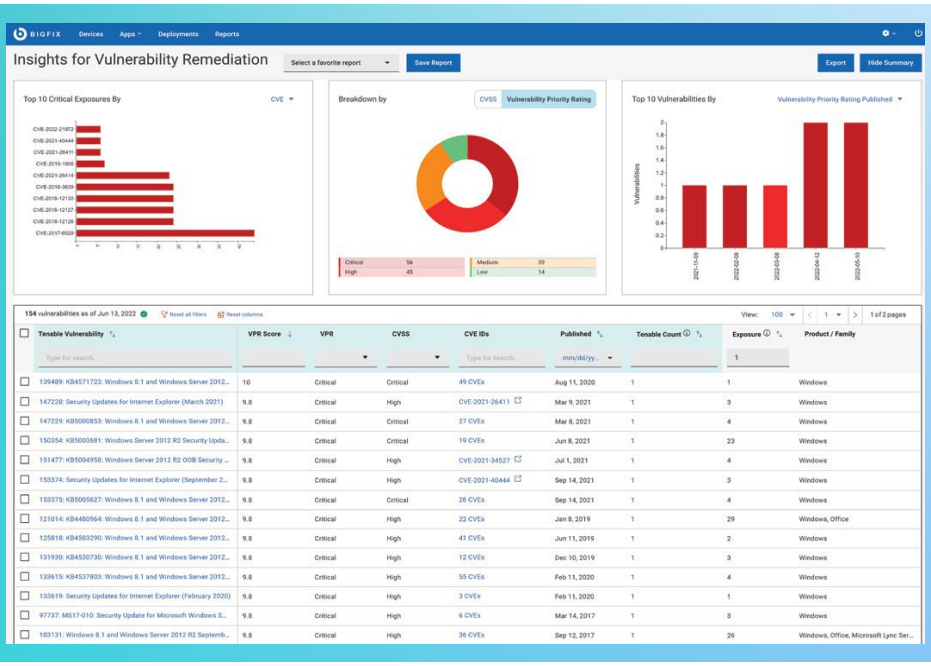
Top 10 Critical Exposures by CVE/Tenable Plugin – The first chart depicts the top ten critical exposures by either CVE or Tenable Plugin ID to help you quickly identify critical vulnerabilities with high exposures that can be remediated by BigFix.

Breakdown by CVSS/VPR – The second chart depicts vulnerabilities with available Fixlets by Tenable's Vulnerability Priority Rating (VPR) or by CVSS. Tenable's VPR enables risk-based prioritization given on-going threat intelligence of vulnerabilities to help you focus on remediating those that matter most and the CVSS

Vulnerabilities by Date Published and Severity – The third chart augments the details provided in the Vulnerabilities by Severity chart. Specifically, this graph adds the date published (i.e. the date the vulnerability record was first added

(2) Data view – Depicts vulnerabilities with available Fixlets, along with the number of affected devices in a tabular format. The data view provides the ability to search each column for a specific value, filter, or sort the values in column. The data view is shown in the bottom half of the image below.

(3) Vulnerability view – From the Data view, select a specific vulnerability to view more detail including vulnerability metadata, available Fixlet content for remediation, applicable devices, and deployment statuses.



Prerequisites

The prerequisites for BigFix solutions are available online at help.hcltechsw.com/bigfix/landing/index.html.

Why BigFix?

The HCL BigFix endpoint management platform helps IT Operations deliver visibility, continuous compliance and intelligent automation to all endpoints, regardless of operating system, location or connection status. It enables streamlined management processes, tool consolidation and operational cost reduction. Unlike complex tools that cover a limited portion of endpoints, the unified architecture of BigFix can effectively manage every endpoint and ensure compliance of all servers, desktops, and mobile devices whether they are in the office, at home or in the cloud. BigFix finds and fixes endpoints faster than any other solution – delivering greater than 98% first-pass patch success rates.

Visit www.hcltechsw.com/bigfix/offerings/products for more information.

For more information

To learn more, contact your BigFix Sales Specialist, BigFix Business Partner, or visit **www.BigFix.com.**

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, Al 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.

© Copyright 2023 HCL
All product names, trademarks and registered trademarks are property of their respective owners