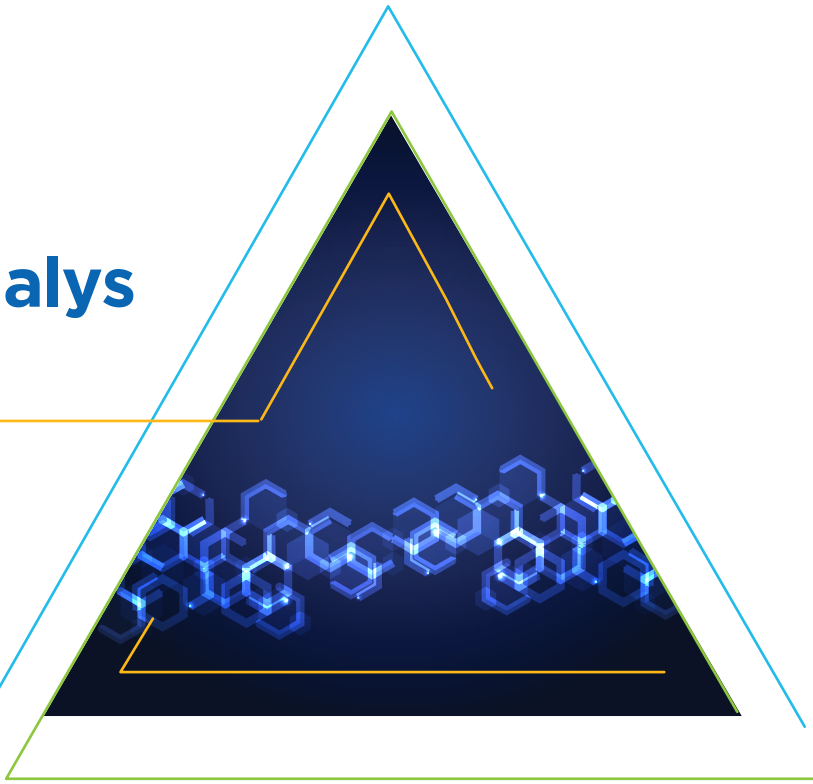
HCL SOFTWARE | BIGFIX

HCL

BigFix Insights for Vulnerability Remediation Integration with Qualys



Align security teams using Qualys® with IT operations teams using BigFix 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 Qualys® 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 Qualys. 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 1/3 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 Qualys 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 Qualys 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 vulnerabilities discovered by Qualys with the recommended remediation Fixlets using the BigFix supersedence engine, while providing the data you need to effectively prioritize remediation actions
- Shrinks attack surfaces and closes the loop between vulnerability detection and remediation
- Requires no additional agents or relays and has no performance impact on the endpoint or network

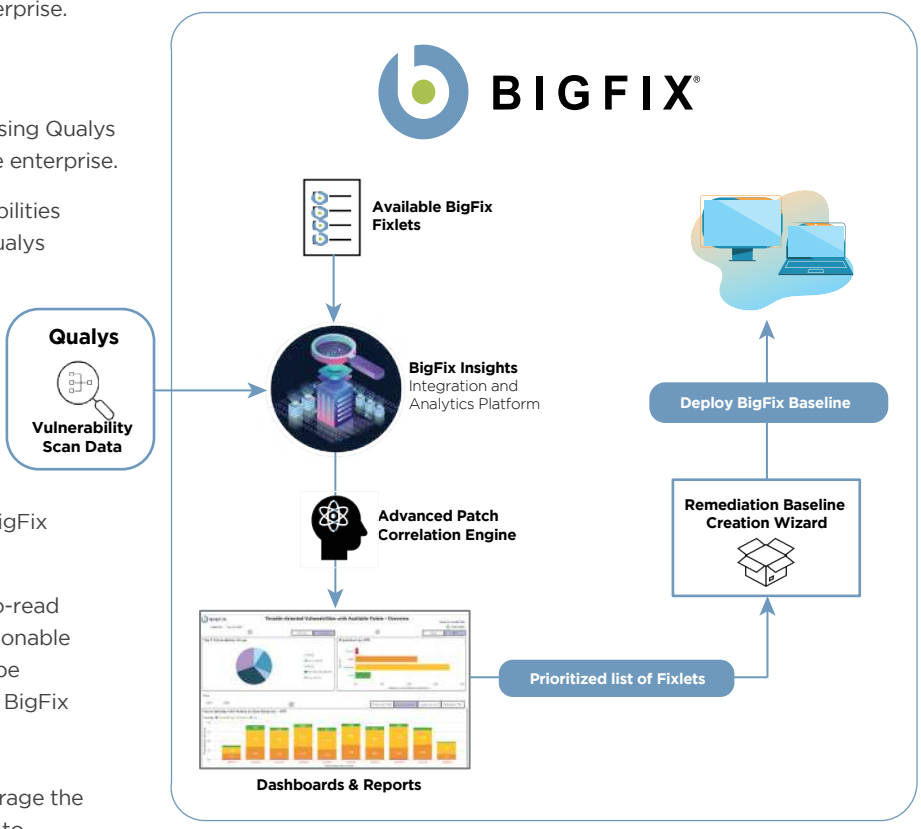
Speed Remediation of Vulnerabilities - How it works

BigFix Insights for Vulnerability Remediation speeds remediation by automating manual processes that are commonly seen in organizations. Automated correlation of vulnerability scan data from Qualys 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 Qualys to identify the vulnerabilities across the enterprise.
2. The vulnerabilities or Common Vulnerabilities and Exposures (CVE®) identified by Qualys 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 automatically correlate the Qualys 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.



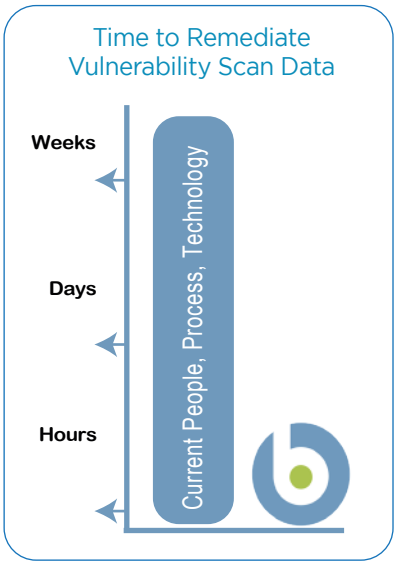
BigFix Insights for Vulnerability Remediation Operational Flow

Using this operational workflow, organizations using Qualys 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

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 no fewer than 4 correlation engines which:

1. Correlate endpoint ID with Qualys endpoint ID
2. Correlate the found vulnerability to a Fixlet
3. Identify and assign the superseded (latest) remediation
4. Correlate the BigFix endpoint to the latest Fixlet



What does this mean in real terms? An organization with 1,000 running vulnerabilities will spend up to 50 person-hours per scan cycle researching and correlating available fixes to the correct assets. With BigFix Insights for Vulnerability Remediation, this time can be reduced to less than 2 hours by automating manual processes and reducing errors and associated rework. Now, an IT organization is able to quickly implement fixes and effectively prove compliance to auditors and executive stakeholders. With BigFix Insights for Vulnerability Remediation, IT Security and IT Operation teams are able to collaborate effectively to quickly remediate vulnerabilities discovered by Qualys, providing significant operational and organizational value to the CIO and CISO. That value is realized through:

- Aligning Security and Operations teams with intelligent automation
- Compressing security vulnerability remediation times by an order of magnitude
- Reducing enterprise security risk.

BigFix Vulnerability Correlation Dashboard

The Qualys-Vulnerability Correlation Dashboard provides actionable views of the correlated data from Qualys 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.

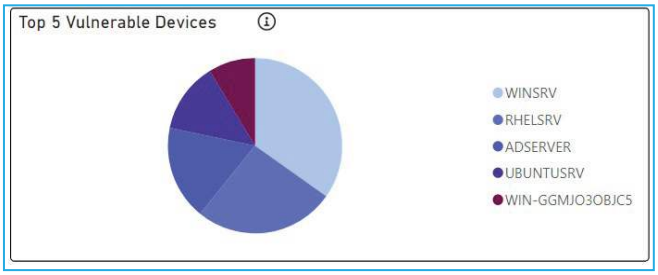
(3) *Vulnerability view* - depicts which devices have a specific vulnerability, and the recommended Fixlet for remediation.

(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. Some leverage Qualys's severity score enabling prioritization of vulnerabilities. Some 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.

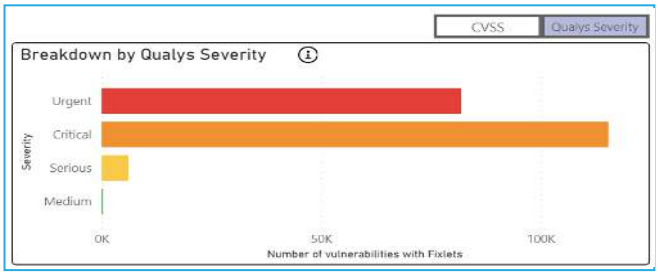
Top 5 Vulnerable Devices

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



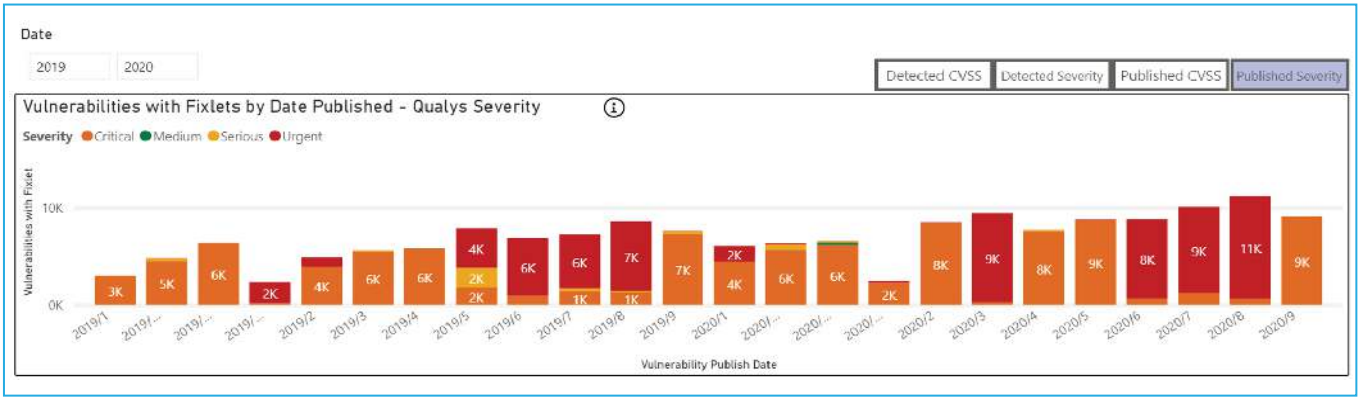
Vulnerabilities by Severity

The second chart depicts vulnerabilities with available Fixlets by Qualys severity score 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 Qualys, 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?

BigFix is built on a unique, highly scalable infrastructure that distributes decision making out to the endpoints. This provides extraordinary functional and performance benefits across the entire BigFix family of solutions while reducing the cost of endpoint management and infrastructure complexity.

BigFix features:

- **A single intelligent agent -** The BigFix agent performs multiple functions, including continuous self-assessment and policy enforcement. It initiates actions in an intelligent manner, sending messages upstream to the central management server and pulling patches, configurations, or other information, to the endpoint in real-time. The BigFix agent self-throttles to 2% CPU, performs dynamic bandwidth throttling to address varying degrees of network bandwidth at remote locations and runs on more than 90 operating systems across Windows, Linux, UNIX, and macOS.
- **BigFix Fixlets™ -** BigFix Fixlets are small units of automation that allow IT operations to simplify their daily operations and focus on more complex operations. BigFix provides more than 500,000 out-of-the-box Fixlets. The BigFix team is continuously updating the Fixlet library, with over 130 content updates per month. BigFix users, business partners, and developers can leverage Fixlets to create custom policies and services for endpoints managed by BigFix. A community library of Fixlets is available on BigFix.me.
- **Highly scalable architecture -** A single BigFix management server can manage up to 250,000 physical and virtual computers over private or public networks, and most implementations require only 1-2 staff per management server. Managed endpoints may include servers, desktops, roaming laptops, endpoints in the cloud, and specialized devices such as point-of-sale (POS) devices, Automatic Teller Machines (ATMs), and self-service kiosks.
- **Multicloud support-** Cloud endpoints can be easily discovered and viewed alongside traditional endpoints using BigFix. Multicloud support allows organizations to deploy the BigFix agent on cloud endpoints for complete visibility, control, and security. It allows organizations to seamlessly manage endpoints running in multiple cloud environments simultaneously – such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform – alongside other endpoints managed by BigFix.
- **Integration options -** BigFix integrates with solutions from major Security and IT Operations technology partners to create a broad enterprise ecosystem. BigFix, alongside its ecosystem partners, delivers a rich set of capabilities to analyze, optimize, gain context and take decisive action across all of your IT operations to increase compliance and reduce cyber risk. Our partners include ServiceNow, IBM, Aruba, Intel, Forescout and others

The BigFix Family

Your investment in BigFix can transform endpoint management, reduce software costs and provide 360-degree visibility. BigFix customers have dramatically consolidated IT tools and endpoint agents, while supporting new work paradigms such as work from home initiatives.

In addition to BigFix Insights for Vulnerability Remediation, the BigFix family includes:

- **BigFix Lifecycle -** Enables IT security and operations to quickly discover, secure, and manage hundreds of thousands of endpoints using a single platform. It provides an automated, simplified patch process that achieves greater than 98% first-pass patch success rates across across Windows, UNIX, Linux, macOS platforms - regardless of location or connection. BigFix Lifecycle also includes OS provisioning, software deployment, remote control, server automation, power management, BigFix Modern Client Management, BigFix Insights, and BigFix Insights for Vulnerability Management.
- **BigFix Compliance -** Continuously enforces endpoint configuration compliance with thousands of out-of-the-box security checks aligned with industry-standard security benchmarks published by CIS, DISA STIG, USGCB and PCI-DSS. BigFix Compliance provides an automated, simplified patch process that achieves greater than 98% first-pass patch success rates across Windows, UNIX, Linux, macOS - regardless of location or connection. BigFix Compliance also includes BigFix Modern Client Management, BigFix Insights and BigFix Insights for Vulnerability Remediation.
- **BigFix Inventory -** Dramatically reduces the time required to conduct a comprehensive software asset inventory for license reconciliation or compliance purposes. It provides valuable information about what software is deployed on endpoints, along with how that software is being used. BigFix Inventory reduces annual software spend, mitigates license non-compliance fines, and helps identify unauthorized or risky software for possible removal.
- **BigFix Modern Client Management -** Enables organizations to have complete visibility and control of Windows 10 and macOS endpoints using either a traditional BigFix agent or Mobile Device Management (MDM) APIs. Leveraging both approaches provide IT teams with the greatest range of management and automation capabilities. Zero touch provisioning speeds and simplifies the deployment of new laptops to remote users. With BigFix Modern Client Management, organizations can more easily manage newer enterprise platforms in a cost-effective way.
- **BigFix Insights -** Enables teams to quickly report their organization's threat posture to executives and perform advanced analysis to drive next steps. This innovative offering provides a powerful endpoint integration platform and database for deeper data insights across traditional on-premise, cloud, and MDM API managed endpoints. BigFix Insights leverages Business Intelligence (BI) reporting tools to provide out-of-the-box and customizable reports.

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.

042021