



Tenable and HCL BigFix Reduce Risk by Optimizing Remediation Workflows



Understanding the most critical vulnerabilities and using that information to match with the right remediation steps is a constant challenge for today's organizations. They lack visibility of their attack surface, are usually guessing to prioritize vulnerabilities using antiquated methods like CVSS and fall short with the proper remediation steps.

Functionally, security teams are tasked with identifying and prioritizing those vulnerability insights and IT operations are responsible for remediating the affected assets. To be effective in reducing cyber risk, these disparate teams need to work in unison. But, they constantly find themselves out of sync, sometimes resorting to inefficient collaboration methods such as email or spreadsheets that lack the proper remediation steps. Even IT ticketing systems fall short as they lack the 'last mile' when it comes to the actual remediation process. The result of these fragmented, manual steps requires a lot of time and resources to keep up with remediation efforts. IT never has the time to be up to date with the most relevant findings that security sends them. This drives the need to optimize remediation workflows by combining the proper security context with automated patch management to tackle vulnerabilities that pose the greatest risk to the business.

SOLUTION

This integrated solution helps organizations to see everything, predict what matters and act to address risk. The result? They can utilize Tenable's deepest and broadest vulnerability coverage in the industry, paired with Predictive Prioritization to focus on what matters most, combined with BigFix to correlate the right remediation to the right vulnerability. This drastically improves overall security, mean time for remediation and patch workflows. Organizations have confidence in knowing they are remediating the most critical vulnerabilities based on prioritization, more effectively and efficiently.

VALUE

- Automatically correlate prioritized vulnerabilities with the right remediation steps.
- Align security and IT operation teams to reduce vulnerability resolution time.
- Save time and free up resources to scan more frequently.
- Sync discovered assets between Tenable and BigFix to improve team coordination.
- Reduce cyber risk by utilizing risk-based prioritization from Tenable.
- Harness the power of Tenable Lumin to further prioritize vulnerabilities for patching based on Asset Exposure Score (AES) and Asset Criticality Rating (ACR).

SOLUTION OVERVIEW



TECHNOLOGY COMPONENTS

- Tenable.ep, Tenable.io or Tenable.sc 5.15+
- Tenable Lumin (Optional)
- BigFix Compliance, Lifecycle or Remediate
- BigFix Insights for Vulnerability Remediation (For Tenable)

KEY BENEFITS

- **Automatically correlate** prioritized vulnerabilities with the right remediation
- **Reduce risk, exposure and loss** with vulnerability remediation
- **Scale and eliminate manual processes**
- **Improve operational efficiency** with coordinated response between Security and IT teams



For more information, contact Carahsoft or our reseller partners:
Tenable@carahsoft.com | 888-662-2724

TENABLE AND HCL BIGFIX REDUCE RISK BY OPTIMIZING REMEDIATION WORKFLOWS

Understanding the most critical vulnerabilities and using that information to match with the right remediation steps is a constant challenge for today's organizations. They lack visibility of their attack surface, are usually guessing to prioritize vulnerabilities using antiquated methods like CVSS and fall short with the proper remediation steps.

Functionally, security teams are tasked with identifying and prioritizing those vulnerability insights and IT operations are responsible for remediating the affected assets. To be effective in reducing cyber risk, these disparate teams need to work in unison. But, they constantly find themselves out of sync, sometimes resorting to inefficient collaboration methods such as email or spreadsheets that lack the proper remediation steps. Even IT ticketing systems fall short as they lack the 'last mile' when it comes to the actual remediation process. The result of these fragmented, manual steps requires a lot of time and resources to keep up with remediation efforts. IT never has the time to be up to date with the most relevant findings that security sends them. This drives the need to optimize remediation workflows by combining the proper security context with automated patch management to tackle vulnerabilities that pose the greatest risk to the business.

SOLUTION

This integrated solution helps organizations to see everything, predict what matters and act to address risk. The result? They can utilize Tenable's deepest and broadest vulnerability coverage in the industry, paired with Predictive Prioritization to focus on what matters most, combined with BigFix to correlate the right remediation to the right vulnerability. This drastically improves overall security, mean time for remediation and patch workflows. Organizations have confidence in knowing they are remediating the most critical vulnerabilities based on prioritization, more effectively and efficiently.

VALUE

- Automatically correlate prioritized vulnerabilities with the right remediation steps.
- Align security and IT operation teams to reduce vulnerability resolution time.
- Save time and free up resources to scan more frequently.
- Sync discovered assets between Tenable and BigFix to improve team coordination.
- Reduce cyber risk by utilizing risk-based prioritization from Tenable.
- Harness the power of Tenable Lumin to further prioritize vulnerabilities for patching based on Asset Exposure Score (AES) and Asset Criticality Rating (ACR).



TECHNOLOGY COMPONENTS

- Tenable.ep, Tenable.io or Tenable.sc 5.15+
- Tenable Lumin (Optional)
- BigFix Compliance, Lifecycle or Remediate
- BigFix Insights for Vulnerability Remediation (For Tenable)

KEY BENEFITS

- **Automatically correlate** prioritized vulnerabilities with the right remediation
- **Reduce risk, exposure and loss** with vulnerability remediation
- **Scale and eliminate manual processes**
- **Improve operational efficiency** with coordinated response between Security and IT teams

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

ABOUT HCL SOFTWARE AND HCL BIGFIX

HCL Software, a division of HCL Technologies (HCL), develops, markets, sells, and supports over 20 product families in the areas of DevSecOps, Automation, Digital Solutions, Data Management, Marketing and Commerce, and Mainframes. Its mission is to drive ultimate customer success with their IT investments through relentless innovation of its products. HCL BigFix is the only endpoint management platform that enables IT Operations and Security teams to fully automate discovery, management and remediation – whether its on-premise, virtual, or cloud – regardless of operating system, location or connectivity. Learn more at www.bigfix.com.

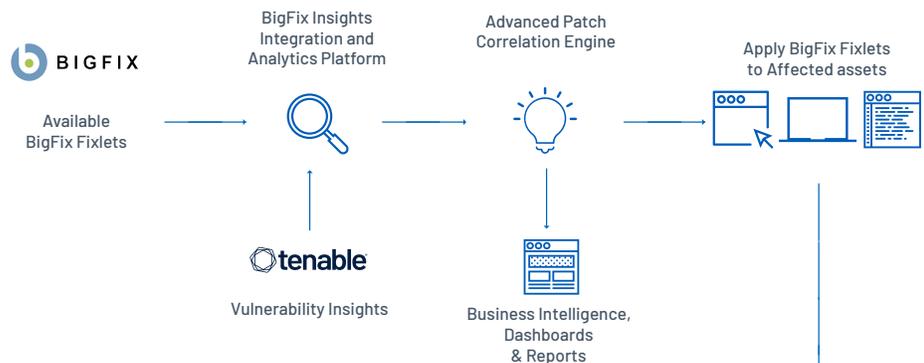
FEATURES

With this integration, you can:

- Align asset data between BigFix and Tenable to identify potential gaps in coverage.
- Automatically sync and correlate vulnerability data from Tenable to BigFix Fixlets.
- Utilize Tenable threat and scoring metrics like:
 - Vulnerability Priority Rating (VPR) for Tenable.io and Tenable.sc
 - Asset Exposure Score (AES) from Lumin within Tenable.io
 - Asset Criticality Rating (ACR) from Lumin* within Tenable.io

HOW IT WORKS

1. Vulnerability insights sync from Tenable into BigFix using the 'BigFix IVR for Tenable' app.
2. Tenable vulnerabilities are combined with BigFix asset data.
3. BigFix users are guided on the best remediations based on discovered vulnerabilities using Fixlets.



Leverage various dashboards and reports for a holistic view of your vulnerability and Fixlet data

For a Tenable product evaluation, please contact: bigfix@tenable.com

This integration is built and supported by Bigfix, for support please visit: <https://www.hcltechsw.com/wps/portal/contact-us>

For Federal support, please visit: <https://www.hcltechsw.com/wps/portal/resources/us-government-contact>



Thank you for downloading this Tenable solution brief! Carahsoft is the distributor for cyber solutions available via NASPO, Quilt, OMNIA, and other contract vehicles.

To learn how to take the next step toward acquiring Tenable's solutions, please check out the following resources and information:



For additional resources:
carah.io/TenableResources



For upcoming events:
carah.io/TenableEvents



For additional Tenable solutions:
carah.io/TenableSolutions



For additional cyber solutions:
carah.io/Cybersecurity



To set up a meeting:
Tenable@carahsoft.com
888-662-2724



To purchase, check out the contract vehicles available for procurement:
carah.io/TenableContracts