HCLSoftware

# HCL BigFix
# CyberFOCUS Security Analytics

Empowering IT Operations to Secure the Enterprise

Organizations are challenged to remediate vulnerabilities with speed. The gap in objectives, tools and processes of security and IT operations results in critical vulnerabilities not being remediated quickly enough to protect the enterprise. HCL BigFix is extending its remediating capabilities so our users can proactively secure the enterprise faster than ever. BigFix CyberFOCUS Security Analytics is a set of security capability designed to help IT Operations collaborate with Security Operations to PRESCRIBE the most effective remediation strategies, PROTECT against exploits and PROVE better cyber security outcomes in real time.

## Prescribe

Simulate the best vulnerability remediation strategies against exploits used by APT groups and show remediation status to the CISA Known Exploited Vulnerabilities catalog.

## Protect

Immediately patch exploitable vulnerabilities from within BigFix including vulnerabilities discovered by Tenable or Qualys correlated with available fixes.

## Prove

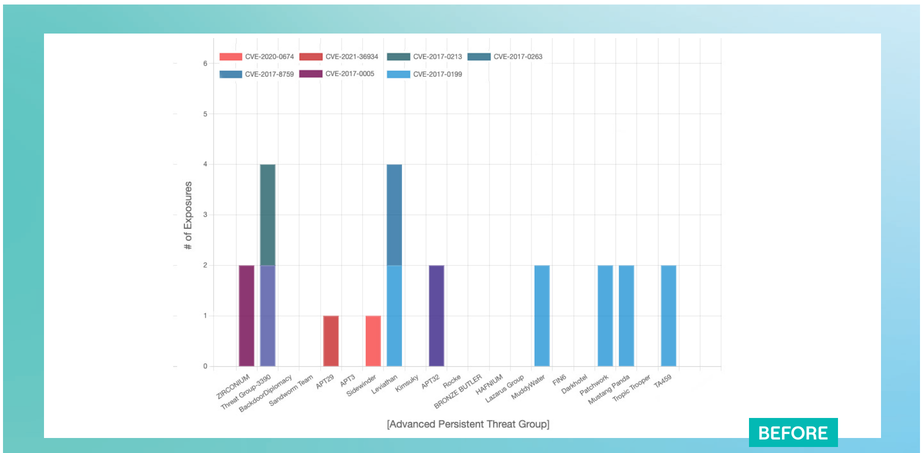
Use Protection Level Agreement (PLA) Analyzer so you can measure and track actual cyber risk reduction using agree-upon targets defined by business stakeholders and IT Operations.

## Advanced Persistent Threat (APT) Mapping and a Vulnerability Remediation Simulator

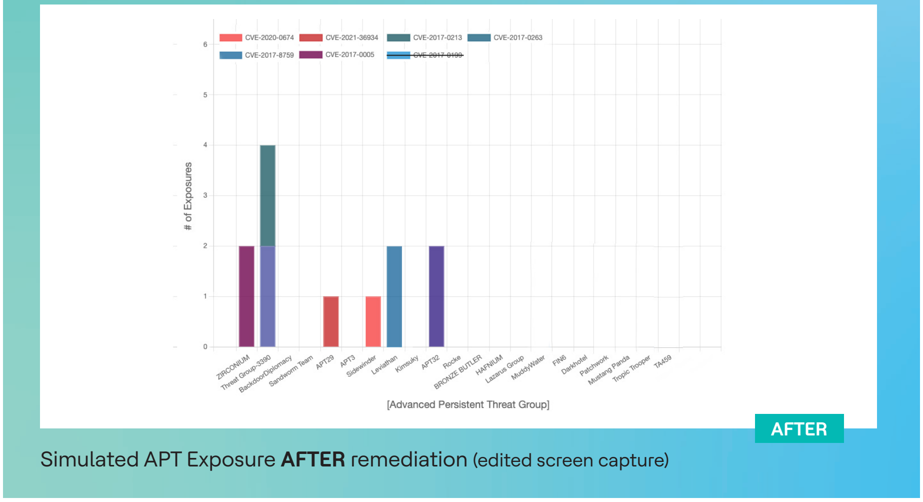
The Vulnerability Remediation simulator displays your recorded, unremediated vulnerabilities, grouped by the most critical exploits used by MITRE APTs. Simulation shows you which remediations will reduce the APT exploit attack surface the most.

Assume a BigFix administrator wants to identify one or more vulnerabilities that, when remediated, will reduce the exploitable attack surface the most. In the top screen capture on the right (the BEFORE image,) the administrator sees all the attack groups present in the environment are shown as well as the number of exposures in each group. Additionally, the administrator sees all the CVEs that are applicable to the environment, represented by the differnet colored bars.

By selecting CVE-2017-0199, the administrator simulates the remediation of that vulnerability and sees the number of exposures are reduced in five different attack groups (shown in the AFTER image to the right.)



Current APT Exposure (edited screen capture)

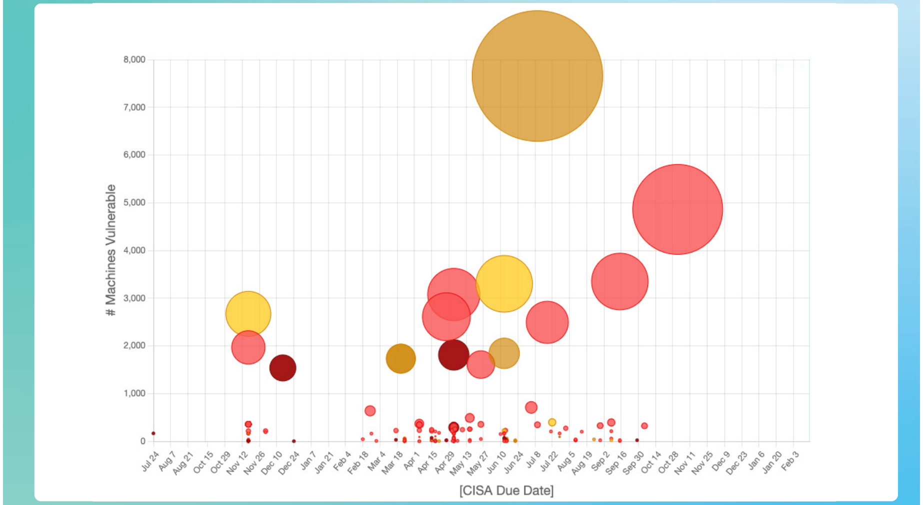


Simulated APT Exposure **AFTER** remediation (edited screen capture)

## BigFix CISA Known Exploited Vulnerability Exposure Analyzer

Another innovation is the BigFix CISA Known Exploited Vulnerability Exposure Analyzer, which maps your remediation history to the constantly updated CISA Known Exploited Vulnerabilities list which defines the most critical threats in the world.

Using the CISA Known Exploited Vulnerability Exposure Analyzer, IT Operations can identify the most urgent and significant security issues. For instance, in the report shown at the right,  the largest, highest and darkest circle represents the greatest, unremediated exposure across multiple dimensions including time.

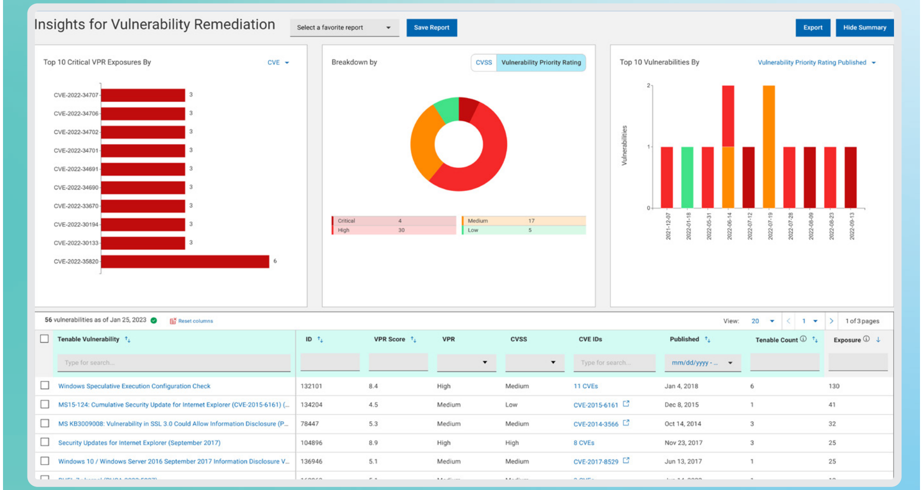


A CISA Known Exploited Vulnerability Report (edited screen capture)

## Vulnerability Remediation

BigFix Insights for Vulnerability Remediation integrates BigFix with vulnerability scan data from Tenable and Qualys. It guides BigFix users on how to apply the best patch and configuration settings to remediate discovered vulnerabilities, and thus reduce risk and improve security.

In the report on the right shows the most critical CVE exposures so user can easily prioritize BigFix remediations. It shows critical exposures sorted by user's choice of filter and sort criteria, overall distribution of exposures by criticality ratings and grouped by priority.

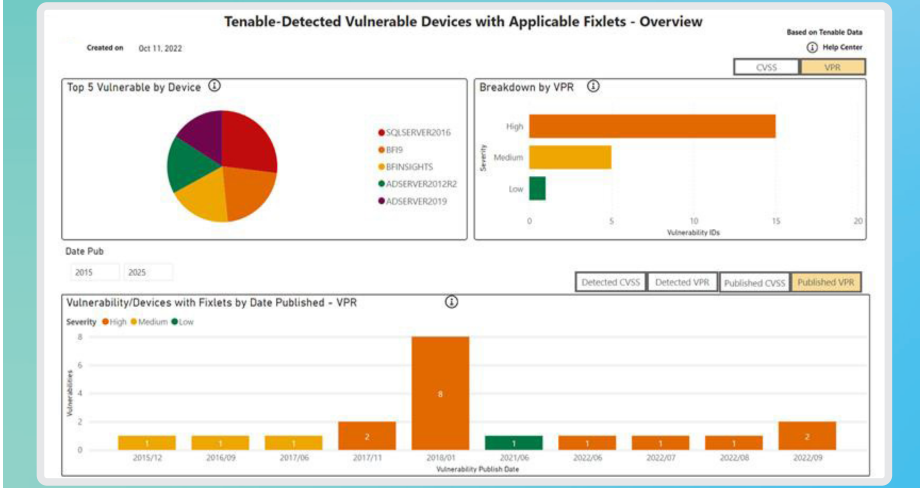


56 vulnerabilities as of Jan 25, 2023 Reset columns View: 20 1 1 of 3 pages

| □ | Tenable Vulnerability | ID | VPR Score | VPR | CVSS | CVE IDs | Published | Tenable Count | Exposure |
|---|---|---|---|---|---|---|---|---|---|
| | Type for search... | | | | | Type for search... | mm/dd/yyyy - ... | | |
| □ | Windows Speculative Execution Configuration Check | 132101 | 8.4 | High | Medium | 11 CVEs | Jan 4, 2018 | 6 | 130 |
| □ | MS15-124: Cumulative Security Update for Internet Explorer (CVE-2015-6161) (... | 134204 | 4.5 | Medium | Low | CVE-2015-6161 | Dec 8, 2015 | 1 | 41 |
| □ | MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (P... | 78447 | 5.3 | Medium | Medium | CVE-2014-3566 | Oct 14, 2014 | 3 | 32 |
| □ | Security Updates for Internet Explorer (September 2017) | 104896 | 8.9 | High | High | 8 CVEs | Nov 23, 2017 | 3 | 25 |
| □ | Windows 10 / Windows Server 2016 September 2017 Information Disclosure V... | 136946 | 5.1 | Medium | Medium | CVE-2017-8529 | Jun 13, 2017 | 1 | 25 |

A Vulnerability Remediation Report

Advanced correlation algorithms aggregate and process the vulnerability data with information from BigFix to drive analytics and reports. The report shown on the right enables IT staff to see correlated vulnerabilities with available fixes and to select which remediations to immediately deploy to substantially reduce the time between discovery and remediation.



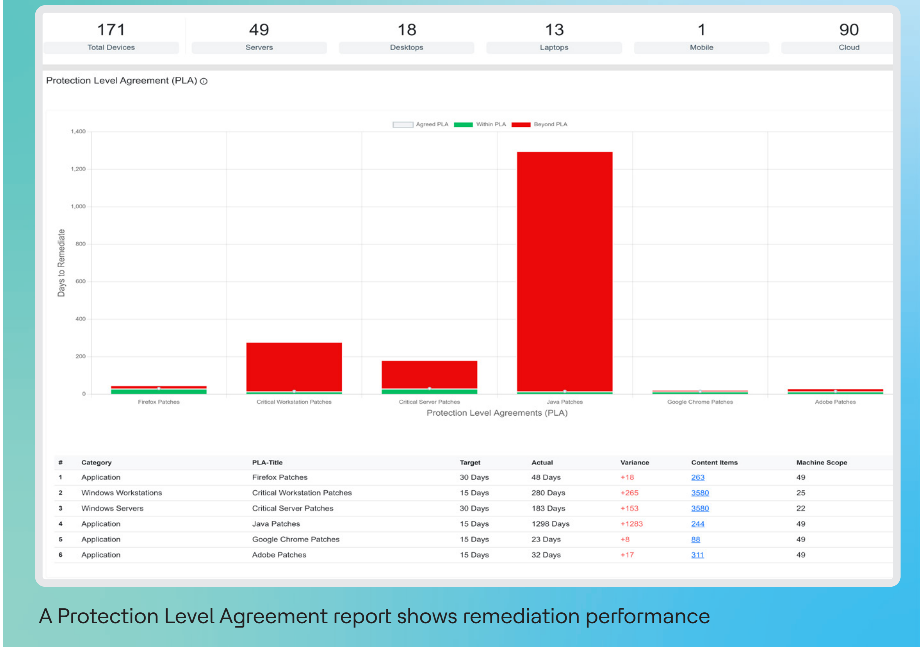
A Tenable-Detected Vulnerablity Device with Applicable Fixes Report

"This is really valuable [for tying IT and SecOps together]. I had no idea BigFix could do that. It's really impressive. How did you do it?"
**– Cybersecurity Specialist, HCLSoftware Business Partner**

## Define and Manage your Protection Level Agreements (PLAs)

BigFix CyberFOCUS Security Analytics introduces a new concept we call Protection Level Agreements. These are a set of baselines that combine asset criticality, CVE criticality, desired patch levels, and compliance standards against agreed-upon service levels defined by business stakeholders and IT Operations.

A Protection Level Agreement report shows remediation performance against six critical areas of vulnerability patching. Green bars show targets that have been met; red bars show missed targets.



| 171 | 49 | 18 | 13 | 1 | 90 |
|---|---|---|---|---|---|
| Total Devices | Servers | Desktops | Laptops | Mobile | Cloud |

Protection Level Agreement (PLA) ⓘ

| # | Category | PLA-Title | Target | Actual | Variance | Content Items | Machine Scope |
|---|---|---|---|---|---|---|---|
| 1 | Application | Firefox Patches | 30 Days | 48 Days | +18 | 263 | 49 |
| 2 | Windows Workstations | Critical Workstation Patches | 15 Days | 280 Days | +265 | 3580 | 25 |
| 3 | Windows Servers | Critical Server Patches | 30 Days | 183 Days | +153 | 3580 | 22 |
| 4 | Application | Java Patches | 15 Days | 1298 Days | +1283 | 244 | 49 |
| 5 | Application | Google Chrome Patches | 15 Days | 23 Days | +8 | 88 | 49 |
| 6 | Application | Adobe Patches | 15 Days | 32 Days | +17 | 311 | 49 |

A Protection Level Agreement report shows remediation performance

## Summary

With BigFix CyberFOCUS Security Analytics, IT Operations can – for the first time – simulate the business impact of Vulnerability Remediation while getting ahead of the biggest threats. They can also take a more collaborative role in enterprise security by defining and measuring their performance in protecting the organization.

BigFix CyberFOCUS Security Analytics is available in BigFix Lifecyle, BigFix Compliance and BigFix Remediate.

For more information contact our federal team at info@hclfederal.com.

## About HCLSoftware

HCLSoftware develops, markets, sells, and supports product families in the areas of Digital Transformation, Data, Analytics & Insights, AI & Automation and Enterprise Security platforms. HCLSoftware is the cloud-native solution factory for enterprise software and powers millions of apps at more than 20,000 organizations, including more than half of the Fortune 1000 and Global 2000 companies. HCLSoftware's mission is to drive ultimate customer success with its IT investments through relentless product innovation.

## Benefits

- Help IT Operations collaborate to PRESCRIBE the most effective remediation strategies, PROTECT against exploits and PROVE better cyber security outcomes
- Minimize business interruptions by simulating the impact of remediating specific vulnerabilities on the enterprise attack surface
- Leverage threat data from MITRE and CISA as well as discovered vulnerablites by Tenable or Qualys to visualize and prioritize exposures across your fleet of endpoints
- Define and measure remediation efforts against agree-to targets defined by business stakeholders and IT Operations using Protection Level Agreements (PLAs)