Rezilion | tenable

SOLUTION OVERVIEW

Tenable Rezilion Integration

THE CHALLENGE

Too many vulnerabilities, not enough resources, and too little time.

As the frequency of new products released rises and as the attack surface keeps growing, most companies are faced with a common problem—a growing vulnerability workload. Their vulnerability scanners report countless vulnerabilities and there is simply not enough resources to fix all of these vulnerabilities, leaving their networks vulnerable and exploitable.

Companies need a solution that is able to validate and prioritize vulnerabilities specific to their environment. This will help determine which vulnerabilities are exploitable and which are not, resulting in companies remediating what matters most to them to increase their security posture.

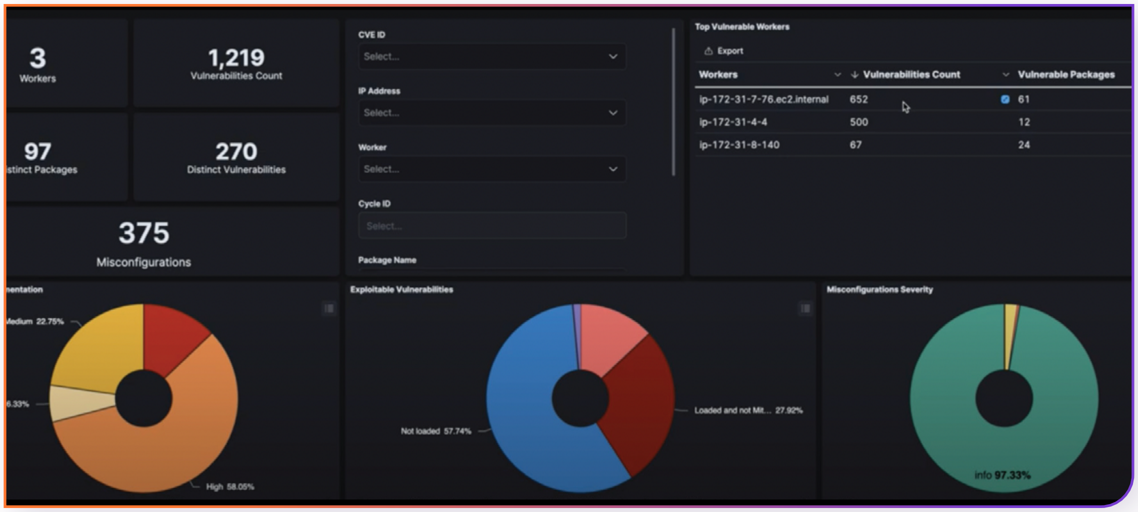
THE VALUE

Know what is exploitable and what to prioritize first in your environment.

The Rezilion integration for Tenable does just that. Using this integration, our customers can understand which vulnerabilities discovered by Tenable are exploitable in the specific runtime context of their environment. The Rezilion platform ingests findings from vulnerability scans performed by our customers. Rezilion takes this feed and validates which vulnerabilities are associated with components that are loaded in memory and exploitable.

A few benefits of this integration include:

- ✓ **85% or more reduction in patching efforts**—Fix what matters most in your environment.
- ✓ **Reduction of remediation timelines from days to hours**—Ensure real threats are addressed in a timely manner.
- ✓ **Dynamic Software Bill of Materials (SBOM)**—Create a dynamic inventory of your environment, including OSS and other elements present in your software package, which allows you to track them in real time.
- ✓ **Drive security automation**—A simple API integration to automatically validate vulnerabilities reported by Tenable IO.
- ✓ **Prioritize risk**—Granular mapping of exploitable vulnerabilities by file, library, and asset to prioritize effort on the biggest risk.
- ✓ **Highlight coverage gaps**—Correlate scans across the fleet and report assets with and without vulnerability scan data to flag coverage gaps.



Workers	Vulnerabilities Count	Vulnerable Packages
ip-172-31-7-76.ec2.internal	652	61
ip-172-31-4-4	500	12
ip-172-31-8-140	67	24

Figure 1: What you see here is a dashboard showing a vulnerability feed of Tenable IO using the API-API connector. We validate the vulnerabilities in the Tenable IO feed by showing if the reported vulnerabilities are associated to components that are loaded in memory and are therefore exploitable. In this example specifically, we show three VMs that have Rezilion running and have been scanned by Tenable. Of the vulnerabilities detected, we have validated that—57% of these are associated with components not loaded in memory and therefore unexploitable. NOTE: We also pass through misconfiguration metadata from Tenable for completeness of reporting in the dashboards.

Why this integration matters to the CISO, Product Security, and DevOps

1. SLAs more achievable. The CISO is responsible for overall security risk across the platform. The Rezilion—Tenable integration will reduce mean time-to-patch, which helps to reduce risk and make

2. The product security team aims to drive risk reduction. The integration to the Rezilion platform will highlight gaps in scan coverage and validate risk disclosed by Tenable.io scans in near real time with minimal effort.

3. DevOps personnel are responsible for validating and remediating risk within defined SLAs, usually based on vulnerability severity. The Rezilion—Tenable integration will reduce effort associated with manually validating vulnerabilities, allowing DevOps to reduce the effort associated with patching by ~85%.`

Why is This Integration Important?

Customers who use Rezilion and Tenable would benefit from this integration as it helps them validate the true risk of the scan findings and prioritize the findings that pose the greatest risk and reduce patching efforts by 85%.

KEY FEATURES:

1. **Automatic ingestion of scan findings at a configurable frequency**

2. **Validation of vulnerability findings to assess exploitable risk.**

3. **Visual display of results in interactive dashboards that are exportable and provide detailed drill-downs for analysis.**

4. **Prioritized list of vulnerabilities validated as exploitable and mapped to software components and assets for remediation planning.**

5. **Prioritized list of vulnerabilities validated as exploitable and mapped to software**

ABOUT REZILION Rezilion's platform automatically secures the software you deliver to customers. Rezilion's continuous runtime analysis detects vulnerable software components on any layer of the software stack and determines their exploitability, filtering out up to 95% of identified vulnerabilities. Rezilion then automatically mitigates exploitable vulnerabilities across the SDLC, reducing vulnerability backlogs and remediation timelines from months to hours, while giving DevOps teams time back to build.

Learn more about Rezilion's software attack surface management platform at www.rezilion.com and get your 30 day free trial.

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 or try tenable at https://www.tenable.com/products/tenable-io/evaluate.

Get Started with Rezilion Solutions. Visit us on AWS Marketplace or www.Rezilion.com to request a demo or purchase today.