Rezilion

SOLUTION BRIEF

Software Supply Chain Security

WITH REZILION'S SOFTWARE ATTACK SURFACE MANAGEMENT PLATFORM you can automatically identify your third-party and Open Source Security (OSS) components, know whether they are exploitable, and map their journey throughout the product lifecycle and technology stack for a holistic understanding of your supply chain risk and secure the software you deliver to customers.

Why Use Rezilion

1. **Full-stack,** full-cycle visibility into your third-party and OSS components
2. **Get** detailed information on all the components from exploitability to provenance
3. **Prioritize** and automatically remediate your supply chain vulnerabilities
4. **Release** with confidence knowing only secured components are shipped to production

Key Features

- **Know** your open source components
- **Know** what's exploitable
- **Track** compliance to open source licenses
- **Map** your component journey from development to production

How the Platform Works

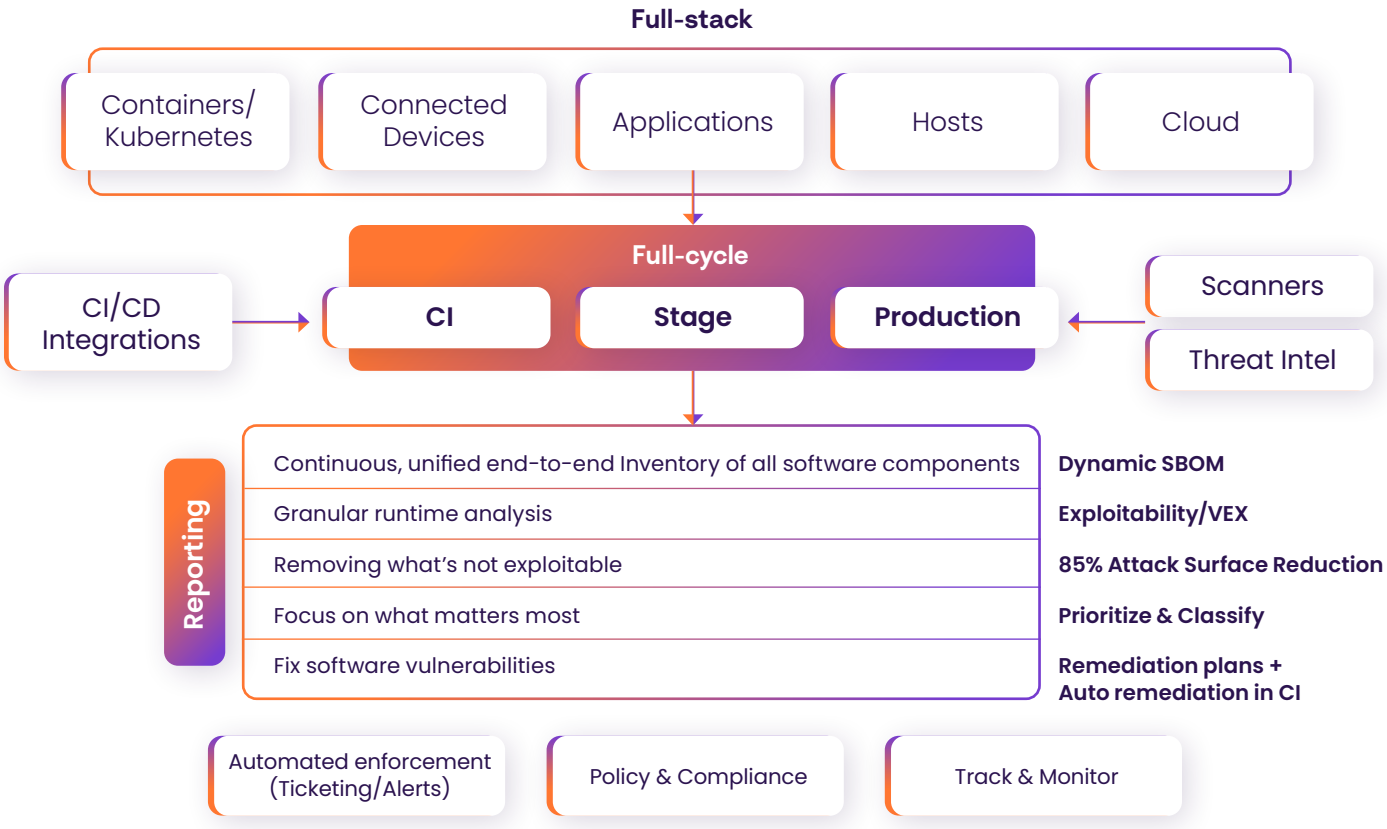
Rezilion platform secures your software in three easy steps:

- **Discover:** Rezilion's Dynamic SBOM discovers and identifies all software components on any layer of the software stack and at any stage of the Software Development Life Cycle (SDLC).
- **Prioritize:** Using continuous granular runtime analysis the platform detects vulnerable software components and determines their exploitability- filtering out 85% of vulnerabilities.
- **Remediate:** Rezilion then automatically mitigates exploitable vulnerabilities across the SDLC from CI to production, reducing vulnerability backlogs and remediation timelines from months to hours.

With this holistic software attack surface management approach Rezilion customers can:

- **Save** countless hours they would otherwise spend on fixing all of the vulnerabilities including ones that do not pose a risk
- **Shorten** attack windows
- **Give** DevOps teams time back to build
- **Improve** their time to market by releasing products quickly and securely

Rezilion's Software Attack Surface Management Platform



Jobs to be Done

1. **Create** and maintain an inventory of all the OSS components used in your software with Rezilion's Dynamic SBOM
2. **Export** your Dynamic SBOM in CycloneDX format for easy sharing with customers, auditors, and other stakeholders.
3. **Quickly search** and find vulnerable OSS components, know if they are actually loaded to memory, and understand the risk associated with them.
4. **Manage** open source license compliance by identifying and fixing out-of-compliance software.
5. **Track** the spread of vulnerable components from CI/CD pipeline, to apps, to production, and know where each component is to better manage the software supply chain risk.
6. **Create** and enforce consistent security policies to assure that only secured components are shipped to production.

Get Started with Rezilion Solutions Learn more about Rezilion's software attack surface management platform at www.rezilion.com and get your 30-day free trial. Or see our platform in action and book a demo at https://www.rezilion.com/request-a-demo/.

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.