

Software Supply Chain Security



WITH REZILION'S SOFTWARE SUPPLY CHAIN SECURITY 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

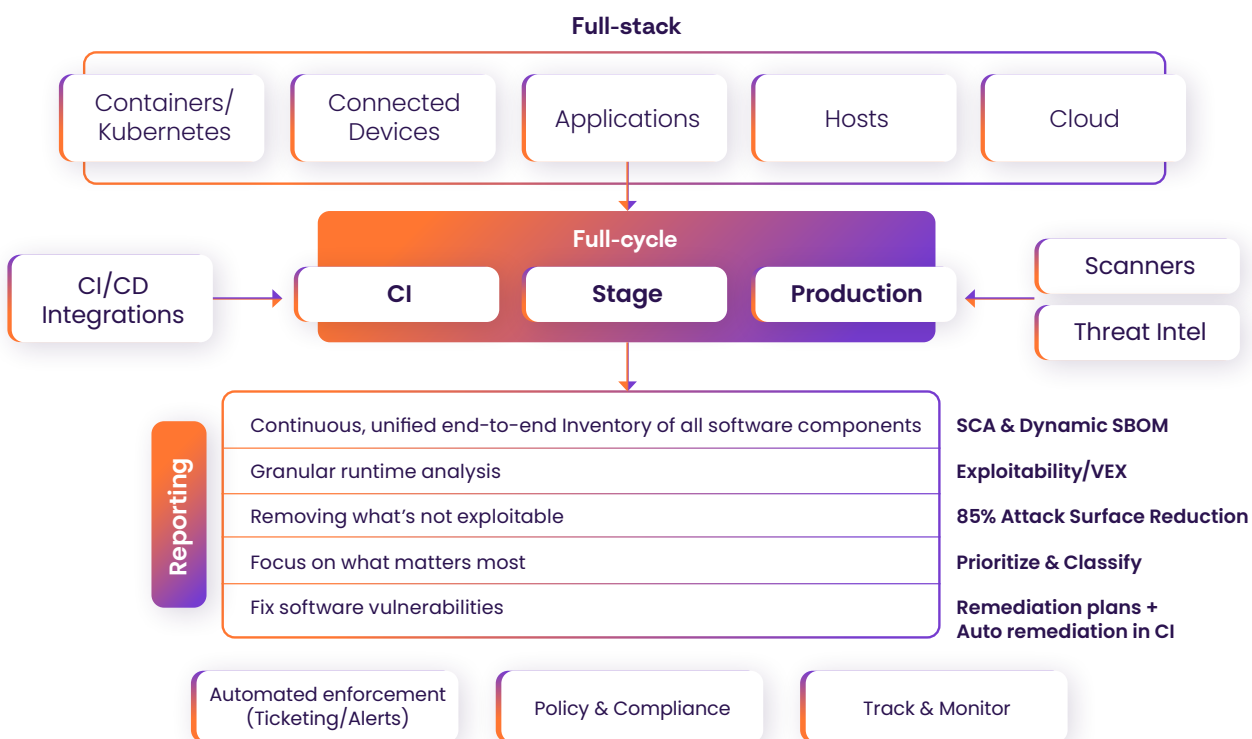
Rezilion platform secures your software in four easy steps:

- ✓ **Discover:** Create an instant inventory of all the software components in your environment with Rezilion's SCA and Dynamic SBOM
- ✓ **Aggregate:** Enrich and consolidate scan results from multiple tools in a single dashboard for a complete view of your software attack surface
- ✓ **Prioritize:** Using continuous granular runtime analysis the platform detects vulnerable software components and determines their exploitability — filtering out vulnerabilities that pose no risk (up to 85%)
- ✓ **Remediate:** Cluster vulnerabilities to eliminate multiple problems at once and automatically execute remediation work to save teams time

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

- ✓ **Easily** aggregate all their third-party and open-source software risk
- ✓ **Save** countless hours they would otherwise spend on fixing all of the vulnerabilities, including ones that do not pose a risk
- ✓ **Shorten** attack windows
- ✓ **Manage** supply chain risks from a single, centralized control panel
- ✓ **Give** DevOps teams time back to build
- ✓ **Improve** their time-to-market by releasing products quickly and securely

Rezilion's Software Supply Chain Security Platform



Jobs to be Done

1. **Create** and maintain an inventory of all the OSS components used in your software with Rezilion's SCA and Dynamic SBOM capabilities.
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. **Know** what's malicious. Leverage threat intelligence to detect malicious software components in your software supply chain.
6. **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.
7. **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 supply chain security 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 software supply chain security platform automatically assures that the software you use and deliver is free of risk. Rezilion detects third-party software components on any layer of the software stack and understands the actual risk they carry, filtering out up to 95% of identified vulnerabilities. Rezilion then automatically mitigates exploitable risk 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 platform at www.rezilion.com and get a 30-day free trial.