

Rezilion Software Attack Surface Management Platform



REZILION'S PLATFORM AUTOMATICALLY SECURES THE SOFTWARE YOU DELIVER TO CUSTOMERS FROM DEVELOPMENT TO PRODUCTION. THE REZILION PLATFORM identifies, prioritizes, and automatically remediates software vulnerabilities across the entire technology stack from containers, cloud workloads, and applications to connected devices providing customers with a holistic software attack surface management solution.

Why Use Rezilion

1. **Access** a unified view into all of your software components with our Dynamic SBOM
2. **Get** a granular understanding of your exploitability with a next-generation vulnerability database
3. **Know** your true software attack surface with runtime validation and eliminate up to 85% of your software vulnerabilities
4. **Eliminate** blind spots with continuous full-stack, full-cycle coverage
5. **Prioritize** and automatically remediate your software vulnerabilities
6. **Define** and automate policy and SLA compliance

Key Features of the Platform

- ✓ **Deployable** in minutes as a plugin to your existing workflow
- ✓ **Single platform** for dev and production
- ✓ **Native** out-of-the-box integrations make it seamless
- ✓ **Dynamic**, searchable, customizable, and exportable dashboards
- ✓ **Share** and collaborate with teams across products and BU's

How the Platform Works

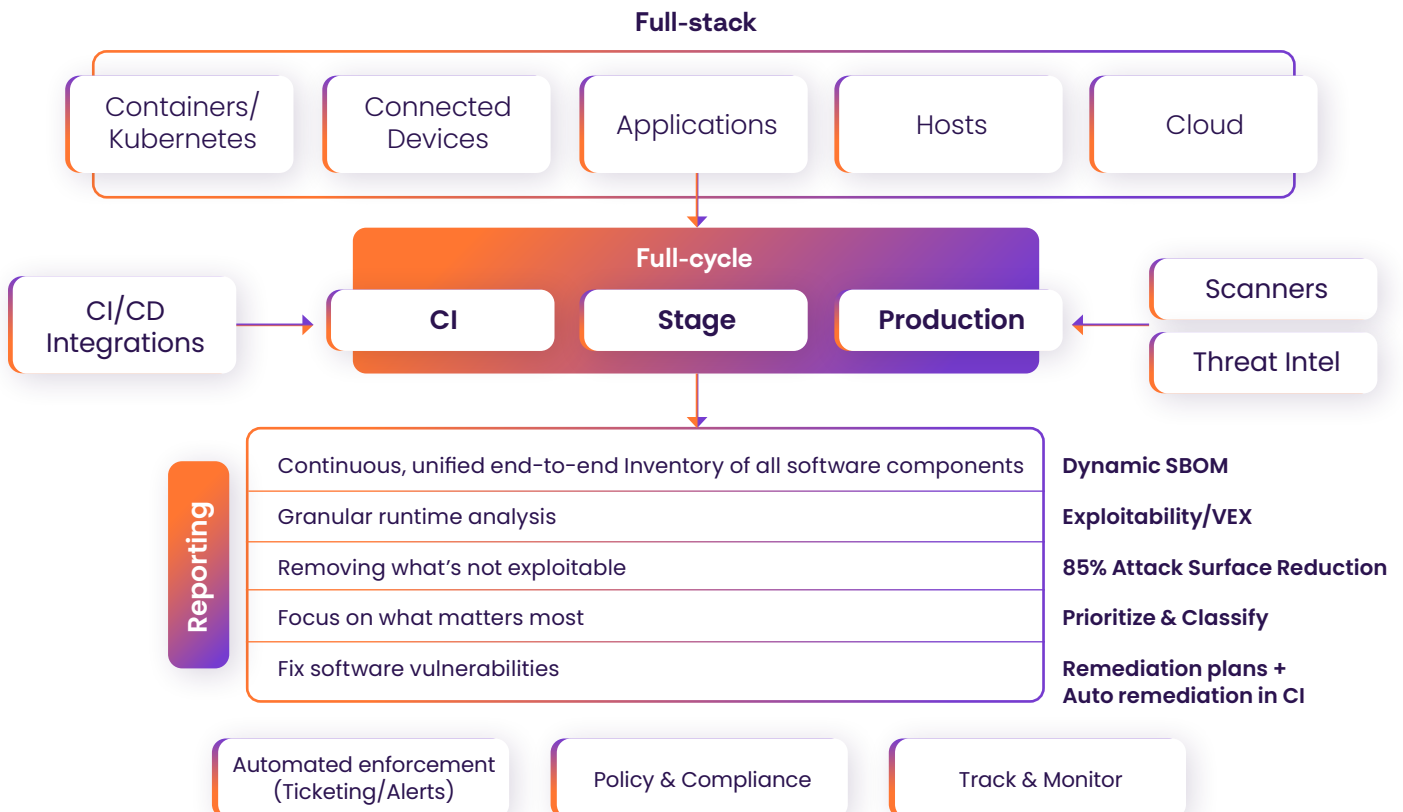
Rezilion platform secures your software in three easy steps:

- ✓ **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:

- ✓ **Easily** view all vulnerable components
- ✓ **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
- ✓ **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





Key Use Cases

- ✓ **Unified view of your software environment**
 - across the entire tech stack and DevOps lifecycle of all scans, software components, vulnerabilities, and supply chain security issues
- ✓ **Integrate** with your existing vulnerability management scanners
- ✓ **End-to-end visibility of your software components** with a Dynamic SBOM
 - Create a live inventory of all software components including open source, in CI/CD, staging, and production environments.
 - Search for any component in your software and know the risks associated with them.
 - Identify and know details of all your open source and third-party components to manage your software supply chain risk.
 - Export and share the Dynamic SBOM in CycloneDX format as well as VEX to fulfill compliance and audit requirements
- ✓ **True Attack surface assessment**
 - Runtime analysis to know what is loaded to memory and what is not
 - Continuous updates
- ✓ **Prioritize and focus on the risk that matters**
 - Deep validation provides a granular understanding of your software attack surface and associated risk
 - Removing 85% of vulnerabilities that are not exploitable
- ✓ **Automated remediation workflows** in CI and production
- ✓ **Manage all your security policies** in one place.
 - Set organizational thresholds of acceptable risk to meet security and compliance requirements.
 - Automatic enforcement of these policies.
 - Continuously monitor security issues and get notified
- ✓ **Full cycle security compliance**
 - Create tickets, patch, and track remediation progress and SLAs using existing workflow management tooling.
- ✓ **Automatically resolve issues** that have been fixed to release developer bandwidth back to innovation work.
- ✓ **Measure and report** on progress with teams across your organization.



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.