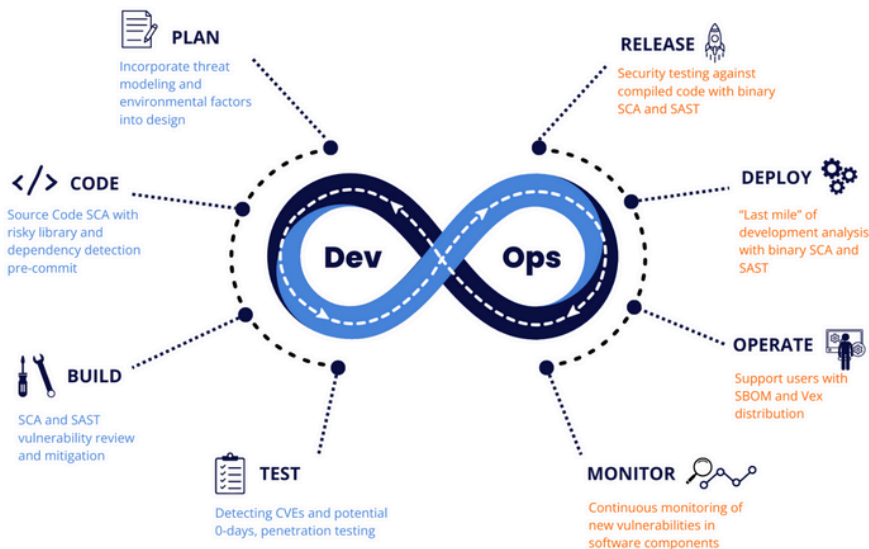


# The Finite State Platform

## Software Supply Chain Security for Connected Products

The rapid growth of connected devices has intensified the need for comprehensive software supply chain security. Governments worldwide are mandating stringent regulations on connected products, from Software Bills of Materials (SBOMs) to vulnerability management and secure-by-design principles. Securing your software supply chain is not just about compliance – it's about staying ahead of threats, protecting your brand's reputation, and ensuring long-term product success.



### Purpose-Built for the Internet of Things and Embedded Systems




Finite State offers a centralized platform for securing the software supply chain of connected products through the DevSecOps lifecycle. Designed to handle the scale and complexity of diverse product portfolios and extensive software ecosystems, our platform detects vulnerabilities in source code, binaries, and third-party components, continuously monitors your entire product portfolio, and suggests developer-friendly fixes for easy software supply chain security and compliance.

### Key Capabilities

- > **Detect** vulnerabilities in source code, binaries, open source software, and third-party components
- > **Manage & Monitor** SBOMs and vulnerabilities throughout a product's lifecycle
- > **Prioritize & Remediate** vulnerabilities in real-time with risk scores, tailored remediation guidance, and 150+ integrations into existing CI/CD pipelines
- > **Comply** with global and industry-specific regulations with automated reporting and audit-ready reports

## Unique Visibility and Analysis – Find What Other Tools Can't

Embedded and connected devices require different technology than modern web applications. Leveraging advanced binary analysis and source code SCA, we can reverse-engineer and analyze complex binary formats to provide insight into firmware, legacy systems, and third-party components.

-  Automatic firmware unpacking and analysis
-  Identify vulnerabilities in proprietary code, vendor-supplied code, COTS software, and open source software and their dependencies
-  Support for 18+ programming languages, 130+ binary formats, and 30+ architectures

## Manage the Full SBOM Lifecycle

From SBOM generation to continuous monitoring and easy sharing, Finite State offers a complete SBOM lifecycle solution that goes beyond compliance to provide real-time insights into your software supply chain.

- > Generate, manage, and validate SBOMs to meet global regulatory requirements
- > Automatically generate SBOMs for any software, firmware, or Infrastructure-as-code (IaC)
- > Ingest, unify, and aggregate SBOMs from multiple suppliers and internal sources
- > Continuously monitor & enrich with vulnerabilities correlated with the NVD and 200+ sources
- > Distribute in SPDX, CycloneDX, and custom formats

## Prioritize and Fix What Matters Most

Our platform offers continuous visibility into your entire product portfolio, monitoring for new threats, providing proactive alerts, and developer-friendly remediation guidance that integrates seamlessly into your existing workflows.

- ✓ Prioritize actions based on exploit availability and severity
- ✓ Remediate with tailored recommendations and automated fixes
- ✓ Continuous monitoring with real-time vulnerability alerts
- ✓ Seamless DevSecOps and product security integrations

**Contact us today for pricing**  
**[info@finitestate.io](mailto:info@finitestate.io)**