Securing the Software Supply Chain: How Finite State Aligns with the S2C2F Framework

S2C2F Requirement	Finite State Solution
Level 1: Minimum OSS Goverance Program	
Scan with known vulnerabilities [SCA-1]	Finite State's advanced SCA capabilities scan software binaries for vulnerabilities, enriching data from 200+ threat intelligence & vulnerability sources.
Scan for software licenses [SCA-2]	Finite State analyzes and identifies OSS components, including license compliance checks.
Inventory of all OSS components [INV-1]	The platform automatically generates a comprehensive Software Bill of Materials for any software, firmware, or Infrastructure as Code, providing a detailed inventory of OSS components.
Manual OSS updates [UPD-1]	Finite State will recommend the version to upgrade the OSS component to and the organization must handle the manual updates.
Level 2: Secure Consumption & Improved MTTR	
Scan for end-of-life [SCA-3]	Finite State can identify OSS components that are past their end-of-life.
Alerts on vulns at PR time [UPD-3]	The platform integrates with CI/CD pipelines to provide alerts on vulnerabilities before deployment.

Level 3: Malware Defense & Zero-Day Detection

Proactive security reviews [SCA-5]

Finite State continuously monitors projects and provides insights for proactive risk management.

Level 4: Advanced Threat Defense

Generate SBOM for rebuilt OSS [REB-3]

The platform automates SBOM generation for both pre-built and rebuilt OSS components.

Implement fixes [FIX-1]

The platform provides remediation guidance, enabling users to patch vulnerabilities effectively.

Our Approach

> **Comprehensive Analysis**: Analyze virtually any type of code or binary - software, firmware, operational technology - regardless of its origin or format.

> **Deep Dive into Complexity**: Dissect even the most tightly integrated, complex software like monolithic and statically-linked binaries.

> **Unmatched Accuracy**: More true positives and fewer false positives, for the most accurate picture of device and connected portfolio risk.

> **Broad Coverage**: Protect your entire connected product portfolio, regardless of complexity or age. From individual components to complete systems, or from legacy products to cutting-edge IoT devices.

Compatibility

We cover a wide range of languages and architectures, including the most popular programming languages (Java, JS, .NET) and those preferred for connected device development (C/C++)