FINITE STATE

Vulnerability Scanning with Finite State

Comprehensive, multi-source vulnerability detection & contextual risk prioritization across the software supply chain

Broad Input Coverage for Modern Product Security

Finite State offers unmatched breadth and depth in vulnerability scanning—purpose-built for modern, complex connected products. Our platform supports ingest and analysis across multiple artifact types:

- **Binaries (Firmware, compiled applications, embedded systems)**
  Industry-leading binary analysis purpose-built for OT & IoT firmware, including support for proprietary formats & custom chipsets
- **Source Code (JavaScript, Python, Java, and more)**
  Scan modern software codebases to identify vulnerable dependencies & misconfigurations
- **SBOMs (CycloneDX, SPDX—with full version tracking and reconciliation)**
  Ingest, enrich, & reconcile existing SBOMs for full visibility across the software supply chain

Finite State's unique ability to correlate findings across these input types ensures that no vulnerability is missed—even in black-box or third-party components. This holistic, multi-format coverage supports a continuous and proactive approach to product security.

Our Proven Tactics & Techniques

Finite State leverages a multi-layered approach to vulnerability scanning that includes:

✓ **Static Binary Analysis:** Extracts & decomposes firmware to identify deeply embedded components & configurations

✓ **Source Composition Analysis:** Scans dependencies & custom code for CVEs & licensing issues

✓ **Configuration & Credential Exposure:** Flags weak default settings, hardcoded secrets, & insecure permissions

✓ **Policy-Driven Workflows:** Enforce risk tolerance levels with automated policy gates in CI/CD environments

✓ **Zero-Day Detection:** Identifies potential buffer overflows, memory corruption, & other risky code patterns via proprietary binary SAST engine

Vulnerability Intelligence that Goes Deeper

Finite State enhances its broad scanning capabilities with equally deep vulnerability intelligence — ensuring every finding is actionable and prioritized. Our enrichment engine synthesizes threat data from 200+ public and private sources, including:

- Public data from NVD, CISA KEV, Exploit DB, GitHub Security Advisories
- Private feeds from leading commercial security vendors
- Industry-specific threat data for IoT, medical, automotive, & critical infrastructure
- Proof-of-Exploit & weaponization signals

This layered intelligence supports more confident decisions — from engineering to executive levels — by delivering not just a list of vulnerabilities, but a clear understanding of their relevance and severity.

Intelligent Prioritization Backed by Real-World Context

Finite State doesn't just flag vulnerabilities—it helps you act on the right ones. Our platform prioritizes findings based on real-world impact and regulatory urgency, cutting through the noise to surface what's truly critical:

- Exploitability & weaponization status, including Known Exploited Vulnerabilities (KEV) Catalogs
- Presence in the field (actual vs. theoretical risk)
- Environmental context (e.g., exposure level, privilege requirements)
- Patch availability & fix effort
- Regulatory relevance (e.g., FDA, CRA, Cyber Trust Mark)

This ensures your team focuses on what's actually urgent—not just what's noisy.

Why Finite State?

	Finite State	Black Duck	Netrise	Cybeats
Binary & Source SCA	✅	❌	❌	❌
Firmware-Aware Analysis	✅	⚠️	✅	❌
Exploit Intelligence & VEX	✅	❌	✅	⚠️
Regulatory Readiness	✅	❌	⚠️	✅
Developer Integration (CI/CD)	✅	✅	❌	❌

Differentiator: Built-In Threat Intel + Actionable Output

Finite State doesn't just flag vulnerabilities—we contextualize, score, and recommend:

- SBOMs you can trust: high-fidelity output with clear sources (binary, source, or both)
- Machine-readable risk insights integrated into CI/CD pipelines
- Exportable reports aligned with FDA, EU CRA, & NIST standards
- Auto-generated VEX data to minimize unnecessary disclosures
- Support for version tracking & differential SBOM comparison

Get visibility. Reduce risk. Meet compliance.

Talk to us about a live demo using your firmware or SBOM today.