FINITE STATE

Precision Risk Reduction for Connected Devices

The Challenge

Every firmware scan can return hundreds, or thousands, of vulnerabilities. But not every CVE is exploitable. Traditional tools treat them all the same, forcing teams to waste valuable time chasing false positives and unreachable code paths.

Finite State changes that with Reachability Analysis and Auto-Resolve, a powerful combination that helps product security teams cut through the noise, focus on real threats, and respond at scale.

Reachability Analysis: *Focus on Real, Exploitable Vulnerabilities*

By analyzing firmware binaries with advanced disassembly, control flow analysis, and kernel configuration heuristics, Finite State identifies which vulnerabilities are:

- Potentially Reachable → Prioritize and remediate
- Likely Unreachable → Deprioritize with confidence

Each assessment includes supporting evidence, helping teams validate results and drive smarter remediation decisions.

How it Works

- Binary-level disassembly & static analysis
- Vulnerable function detection
- Call graph & linking type analysis
- Kernel module heuristics
- Curated exploit intelligence

> It's one thing to say, 'Here's 100 CVEs.' It's another to say, 'Only 3 are exploitable in your device.' That's what Reachability gives you: focus.
>
> Roland Lindsey, Sr. Solutions Engineer, Finite State

Auto-Resolve: *One-Click Resolution for Unreachable Vulnerabilities*

Eliminate hours triaging findings that pose no risk and automatically resolve unreachable findings with a single click. Unreachable findings are instantly updated with appropriate VEX status, clearing out noise and bringing clarity to your risk posture.

Key Benefits

- Save time: Eliminate repetitive triage tasks
- Reduce noise: Instantly close unreachable CVEs
- Improve compliance: Generate defensible VEX documentation
- Scale efficiently: Manage growing finding volumes without more headcount

Why It Matters

Precision Risk Reduction
Cut through CVE overload. Focus remediation on what's actually exploitable in your specific environment.

Regulatory Confidence
Support CRA, Cyber Trust Mark, and other frameworks with evidence-based justifications for unpatched CVEs.

Efficient, Scalable Workflows
Reachability + Auto-Resolve drastically reduce triage workload, freeing teams to act on high-priority threats.

Embedded-First Intelligence
Finite State's analysis is built for embedded systems—RTOS, proprietary firmware, and kernel modules—not just web apps.

~90%
reduction in irrelevant alerts

≤15 min
to first results

30–60%
fewer fixes to remediate

0
critical findings overlooked

Unified Product Security: One Platform. Zero Blind Spots

Scan
Gain instant, unified visibility into every component of your software — source code, binaries, open source libraries, and third-party firmware — so nothing is missed.

Prioritize
Use AI-powered Reachability Analysis and exploit intelligence to focus only on vulnerabilities that are truly exploitable, while Auto-Resolve clears out unreachable findings in a single click.

Fix
Accelerate remediation with automated pull requests, guided patches, and real-time validation to ensure fixes are safe, effective, and don't break your build.

Certify
Automate SBOMs, policy enforcement, & audit-ready reporting & stay compliant with global regulations at every stage.

Want to accelerate triage, streamline compliance, and secure your connected products at scale?

Book a demo today