FINITE STATE

The Finite State Platform

Automated Product Security for Connected Devices

@FiniteStateInc
/company/FiniteState
www.finitestate.io

Overview

Finite State provides a unified, flexible, and scalable cybersecurity platform that is purpose-built to safeguard the firmware security posture of connected devices and embedded systems found in the majority of today's IT and OT networks.

Using Finite State, device manufacturers can detect, analyze, and remediate hidden risks found in those connected devices and embedded systems used in enterprises, healthcare, utilities, critical infrastructure, automotive, manufacturing/ICS, and government agencies. Organizations that employ Finite State will improve device security, comply with standards and regulations, and manage and mitigate their supply chain risk while maintaining a high security posture—all through a unified, easy to use, automated platform.

Key Differentiators

Automated product security
Automate the entire device security testing process, reducing or eliminating the need for manual testing tools and processes.

Purpose-built for devices
Product security analysis designed for connected devices and embedded systems. Provides a holistic view of risk present in a device and its supply chain.

Unified platform
A unified platform for both device and supply chain security needs utilizing Device Composition Analys and Binary SAST.

Easy to interpret risk
Actionabe insights designed to make managing risk easier and faster.

Comprehensive SBOMs
SBOM generation that is fast, automated, machine-readable, and covers the ENTIRE device. Provides complete visibility into all device components including firmware versions.

Deep Firmware intelligence
By employing a proprietary firmware intelligence engine comprising 300,000 analyzed firmware images, Finite State offers actionable insights and remediation guidance rooted in real world data.

Easy search
Quickly access all device related information such as vendors, vulnerabilities, firmware versions.

How It Works

Finite State provides a unified, flexible, and scalable cybersecurity platform that is purpose-built to safeguard the firmware security posture of connected devices and embedded systems found in the majority of today's IT and OT networks.

Using Finite State, device manufacturers can detect, analyze, and remediate hidden risks found in those connected devices and embedded systems used in enterprises, healthcare, utilities, critical infrastructure, automotive, manufacturing/ICS, and government agencies. Organizations that employ Finite State will **improve device security, comply with standards and regulations, and manage and mitigate their supply chain risk** while maintaining a high security posture—all through a unified, easy to use, automated platform.

The Finite State platform uses **Device Composition Analysis (DCA)** in combination with proprietary firmware intelligence and public vulnerability sources to assess final packaged firmware present in connected devices.

The platform enables security teams to manage risk and improve product security posture by:

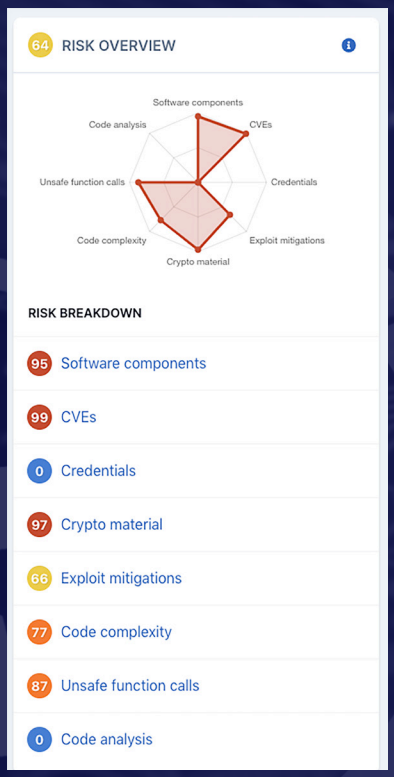
- **Providing a unified, holistic and actionable view into all device security issues.**
- **Scaling across all products and business units to ensure no device security issues are missed that might have an impact on an organization's overall security posture.**
- **Providing visibility into device composition from hardware to applications.**
- **Allowing organizations to understand the contextual risk ecosystem-analytics and gaps.**
- **Helping prioritize remediation of vulnerabilities and security issues.**
- **Ensuring compliance to key industry standards.**
- **Verifying and tracking all vendors to help manage supply chain risk.**

What is Device Composition Analysis?

You can think of DCA kind of like Software Composition Analysis (SCA) used in app development, except that DCA is compatible with the embedded systems and architectures found in connected devices. DCA enables you to uncover and track all third party components in your devices as well as their software licenses and vulnerabilities.

FINITE STATE

Key Features

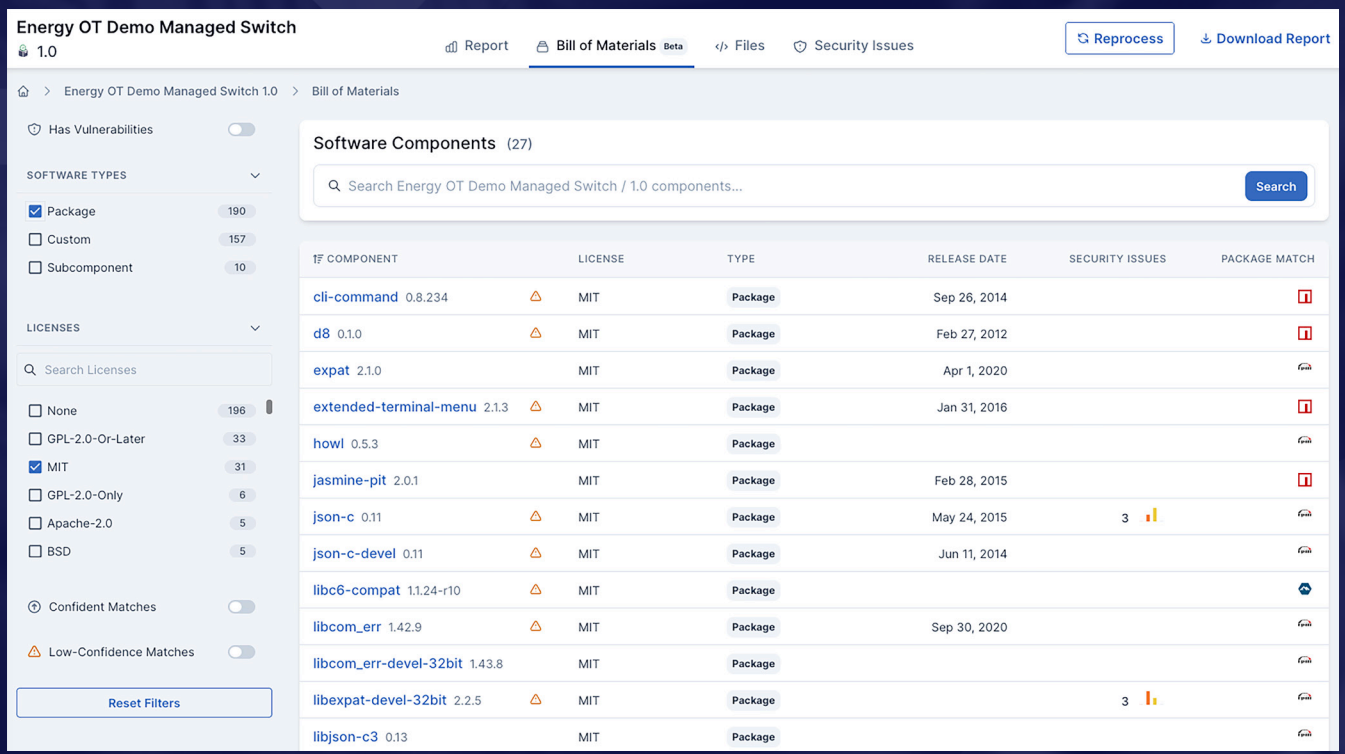


Comprehensive Risk Profile

A unified view of product and supply chain risks with scoring that indicates level of urgency.

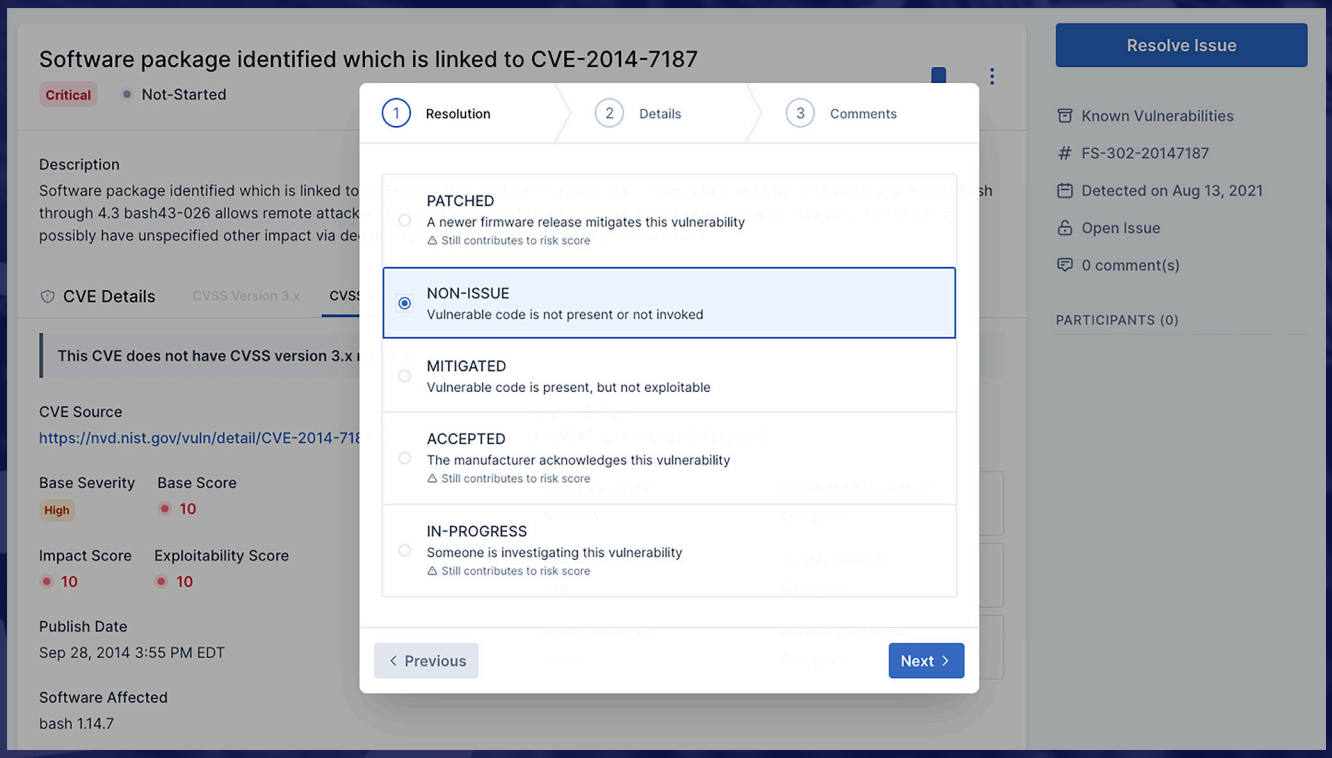
Device Composition

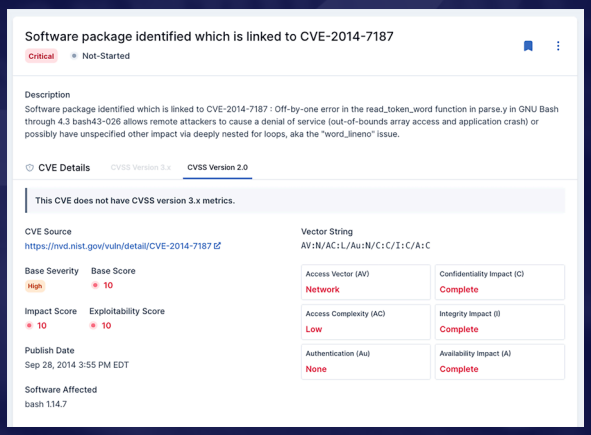
- **Software Bill of Materials (SBOM):** Full visibility into all hardware and software components such as binaries, libraries, open source software (OSS), third-party (3rd) components, embedded software, drivers, etc.
- **Third party and open source risk:** Security risks inherited by vendors and suppliers, including legal risk from unknown, undisclosed, or expired licenses.
- **Weakness and vulnerability detection:** Insecure configurations, hard coded credentials, cryptographic materials, and other possible sources of weakness.



FINITE STATE

Key Features





Issue Management

A way to quickly prioritize and manage security issues. Reduce friction between development teams and product security teams by providing remediation guidance with the largest risk reduction ROI.

Compliance Guidance

Critical information necessary to identify compliance gaps and meet key industry standards and regulations.

Reporting and Analytics

Share insights and analytics with internal and external stakeholders via our easy and robust reporting function.

FINITE STATE

The Complete Product Security Picture

In a comprehensive product security program, traditional AppSec tools and the Finite State Platform complement one another to provide a complete picture of security risk.

While AppSec tools can help an organization scan certain individual components, only scanning the compiled firmware image allows you to see how these components (along with configuration files, drivers, bootloaders, and other parts of the firmware ecosystem) work together and what security issues they introduce.

AppSec Vendors	VS	FINITE STATE
Scans application and source code for desktop and server class software.	**Scanning**	Scans devices and firmware.
Piecemeal approach. Vendors have their own proprietary vulnerability databases and rules.	**Vulnerabilities**	**Full context approach.** Detects vulnerabilities in firmware binaries, revealing CVEs, credentials, exploit mitigations, crypto, and more. Leverages open sources and its own database of ~300,000 firmware images. Detects vulnerabilities in operating systems.
Desktop and server class architectures.	**Instruction Set Architecture**	All architectures.
Incomplete SBOM. Doesn't find libraries that were recompiled or modified. Only focuses on visible source packages and misses out on vulnerabilities (which end up in the binary).	**SBOM**	Comprehensive SBOM of open source, custom/first-party, third-party/COTS components.
Depends on the product type. In SAST, there are binary scanners as well as source code scanners. DAST scanners analyze running application. IAST analyzes bytecode.	**Code Analysis**	Analyzes compiled binaries in firmware.
Separate products for Software Composition Analysis (SCA) and custom code analysis.	**Analysis Type**	Performs Device Composition Analysis (DCA). DCA is Finite State's proprietary methodology to unpack the firmware in the entire device.
Only effective for specific languages. Mixed programming languages lead to unrecognized security issues.	**Programming Language**	Language agnostic, captures all security issues as long as binary runs.

By only scanning source code, you are missing vulnerabilities in open source and third party code, which make up 80–95% of device components on average.

DCA can and should be performed throughout the development lifecycle in order to avoid delayed releases and mitigate security issues early in the process.