AUTOSAR Analysis

FINITE STATE

Deep Visibility Into Automotive Software Supply Chains

AUTOSAR powers modern automotive software — but its complexity and vendor-specific variations often leave OEMs and suppliers blind to what's actually inside their ECUs. Finite State changes that.

Our expanded AUTOSAR capabilities deliver deeper visibility into AUTOSAR components, versions, and configurations, even when source code isn't available. This first release lays the foundation for full AUTOSAR analysis coming in Q1 2026, giving automotive teams the clarity they need to secure their software supply chains.

Key Capabilities

Automatic AUTOSAR Component Detection

Automatically detect AUTOSAR modules, versions, variants, and vendor metadata directly from binaries and configuration files. Gain transparency into how AUTOSAR is implemented across different suppliers and hardware platforms.

Vendor & Version Identification

Where architecture and logging permit, Finite State extracts component versions and vendor details to help teams map vulnerabilities to specific AUTOSAR modules.

More Complete SBOMs

Generate SBOMs that now include expanded AUTOSAR component detail, improving supply-chain transparency and supporting regulatory requirements.

Flexible Scan Inputs

Analyze full project archives, firmware images, or minimal configuration bundles — giving manufacturers control over what data they share without sacrificing coverage.

Expanded Module Coverage (Phase 1)

Identify additional AUTOSAR components and vendor implementations from compiled artifacts — supporting real-world ECU and automotive firmware workflows.

Roadmap: What's Coming

The Q1 2026 release will introduce full AUTOSAR analysis with deeper intelligence, automation, and exploitability insights:

Command Line Tool (CLT) Support
Analyze AUTOSAR files as part of automated pipelines and CI/CD workflows.

Private Vulnerability Advisories
Upload internal advisories to generate custom findings matched to AUTOSAR components and XML metadata.

Configuration-Based Reachability Insights
Use vendor-specific configuration (e.g., Vector DaVinci data) to determine whether vulnerabilities are exploitable based on module settings.

Enhanced Platform Experience
Improved Components and Findings views to highlight AUTOSAR modules, versions, and organization-specific insights for faster triage.

Benefits

Greater Transparency Into ECU Software

Understand which AUTOSAR modules and versions are present across suppliers, platforms, and ECU builds — replacing uncertainty with visibility.

Flexibility for OEM & Supplier Workflows

Scan full builds or minimal configuration sets, enabling collaboration even when suppliers cannot share complete source artifacts.

Streamlined Compliance & Reporting

Meet emerging automotive cybersecurity requirements (UNECE R155, ISO 21434, OEM audit demands) with more complete SBOMs and component-level documentation.

Accelerated Risk & Vulnerability Assessment

Identify where AUTOSAR usage may introduce vulnerabilities — and prepare for advanced exploitability insights coming in Phase 2.

How It Works

Finite State analyzes AUTOSAR-based systems using a combination of binary analysis, configuration parsing, and metadata extraction.

Customers can:

- Upload complete ECU builds for deep analysis
- Provide extracted configuration directories
- Scan through CI/CD using the Finite State CLI (Phase 2)

The platform then maps AUTOSAR modules, vendor variants, and version information to SBOM and findings views, enabling teams to investigate component structures, security gaps, and supplier implementation details.

About Finite State

The Finite State Platform is the AI-First Product Security Platform purpose-built for OEMs and Tier-1 automotive manufacturers. We help teams accelerate secure vehicle software delivery, reduce software supply chain risk, and meet global compliance requirements—all within a single platform that embeds security across the full product lifecycle.

Ready to Secure Everything?

Book a demo to see how Finite State strengthens automotive cybersecurity.