FINITE STATE

The Real Impact of Mature Product Security Programs

Why Maturity Matters

Product security maturity is no longer optional—it's a strategic enabler for connected device manufacturers navigating a fast-evolving regulatory and threat landscape. Mature organizations embed security into every phase of product development and lifecycle management, delivering safer, more resilient products with measurable business benefits.

Six Business Impacts of Strong Product Security Maturity

Faster Time-to-Market
Proactively address vulnerabilities & compliance needs earlier in the development lifecycle to avoid last-minute delays, market access roadblocks, & contract setbacks.

Reduced Remediation Costs
Resolve security issues before release when fixes are faster, cheaper, & less disruptive—minimizing engineering re-work, unplanned downtime, & customer-impacting incidents.

Strengthened Compliance Readiness
Stay ahead of regulations like the EU Cyber Resilience Act, CE RED, FDA 524B, & the US Cyber Trust Mark with built-in SBOM management, risk monitoring, & audit-ready documentation.

Lower Operational Overhead
Eliminate redundant workflows & manual efforts by automating security scanning, SBOM management, & vulnerability correlation across CI/CD pipelines.

Reduced Risk Exposure
Continuously validate your security posture across firmware, APIs, applications, & cloud infrastructure, minimizing the likelihood of breaches, recalls, & legal consequences.

Enhanced Brand Trust & Market Confidence
Demonstrate commitment to security through independent validation, resilient software supply chains, & transparent risk management practices—building trust with customers, partners, & regulators.

> Maturity isn't about checking boxes—it's about embedding security into the DNA of your development and compliance workflows.

Common Security Gaps

SBOM Blind Spots
Incomplete SBOM practices limit visibility into 3rd-party, open-source, & proprietary components, preventing timely detection of known vulnerabilities & license risks.

Pen Testing That Doesn't Scale
Manual, point-in-time pen-testing that's disconnected from the CI/CD pipeline is too slow & too shallow to protect modern, fast-moving product lines.

Lack of Governance
Without a formalized, cross-functional security strategy, teams remain reactive, & compliance becomes a last-minute scramble.

Lack of Standard Security Architectures
Security features & technical controls implemented randomly in the solution without an overall security architecture & strategy make them ineffective.

The Path to Maturity

	What It Means
Governance & Strategy	Align security goals with business priorities & regulatory requirements
Automation & CI/CD Integration	Embed security tooling (e.g., binary SCA, static analysis) into development workflows
SBOM Management at Scale	Automate generation, ingestion, & vulnerability correlation across the product lifecycle
Continuous Pen Testing	Validate security across firmware, APIs, applications, & cloud infrastructure continuously & contextually

Why Finite State

Finite State is the only platform purpose-built to help connected device manufacturers operationalize product security at scale.

With our unified platform and expert-led services, your organization can:

- Generate & manage SBOMs for compliance & supply chain visibility
- Perform deep binary & source-level vulnerability analysis
- Execute scalable, standards-aligned penetration testing (FDA 524B, EU CRA, CE RED)
- Build a security maturity roadmap aligned with your regulatory & business goals