FINITE STATE

Securing your Software Supply Chain

Based on today's supply chain cybersecurity industry drivers and utility regulations; supply chain and cybersecurity teams require specific supply chain analysis capabilities in order to realize the following:

- Reduce penetration testing labor hours by 60%
- Scale software and device penetration testing by 2–5x per year
- Identify previously unknown software and device vulnerabilities and risks
- Effectively manage software supply chain risk

INDUSTRY DRIVERS AND REGULATIONS

- Addressing cybersecurity supply chain risk
- NIST 800-218
- Executive Order 14028

SUPPLY CHAIN AND CYBERSECURITY OUTCOMES

- Improve penetration testing scale and efficiency
- Identify previously unknown supply chain risk
- Expedite vulnerability identification across vendor products

REQUIRED SUPPLY CHAIN CAPABILITIES

- Software package and software bill of material (SBOM) acquisition service
- Automated vendor security analysis of software or firmware
- Software bill of material and vulnerability exploitability exchange enrichment and ingestion
- On-premises platform to ensure compliance with vendor NDAs

Scale Penetration Testing by 2-5x While Reducing Labor Hours by 60%

Finite State provides an automated software and firmware security testing platform which allows supply chain and cybersecurity:

Pen Test Today (Before)	Pen Test with Finite State (After)
Penetration tester have minimal information about the device and/or software package they are evaluating (e.g. black-box testing)	Penetration tester uploads software package to Finite State platform. Within 30 mins to 2 hours the tester receives a list of vulnerabilities, hardcoded passwords, and cryptographic keys within the package.
Testers execute black-box testing and spend **70%** of the time in discovery, enumeration, and scanning activities	Tester now has gray box insights with knowledge of software subcomponents, vulnerabilities, hardcode passwords, and cryptographic keys. They now only spend **30%** of the time in discovery, enumeration, and scanning validation activities
Testers spend **30%** of the time in vulnerability assessment and exploitation	Testers can now spend **70%** of their time on vulnerability exploitation activities. Where available Finite State threat intelligence feeds point the tester to publicly available exploits for each vulnerabilities
Average Time Spent Without Finite State: 1 month	**Average Customer Time Spent with Finite State: 1.5 weeks**

Understand Unknown Software Supply Chain Risk via your Third Party Risk Management (TPRM) Process

Finite State eliminates previously unknown vendor software and product risks by validating vendors' secure software development practices:

TPRM Process Today (Before)	TPRM Process with Finite State (After)
All software and device purchases initiate the TPRM process where the vendor completes a cybersecurity questionnaire	Utility's TPRM process now includes software package and device firmware security testing to validate a vendor's secure software development practices
Vendor fills out a questionnaire with minimal evidence and verification on the security of the actual product and software being procured	Utility TPRM team has actionable data to negotiate new terms or conditions as it relates to the on-going operational costs of securing the vendors' product(s)
Supply Chain Software and Product Risk: UNKNOWN	**Supply Chain Software and Product Risk: Known, reduced, and responsibility pushed back to vendor**

Identify Future "Celebrity" Vulnerabilities in Real Time Across Your Enterprise Product Portfolio

The Finite State Platform includes a software subcomponent repository providing real-time visibility and enterprise search across all vendor software packages and device firmware versions:

VM Today (Before)	VM with Finite State (After)
A high profile or "celebrity" vulnerability is disclosed to the industry (eg: log4j)	A high profile or "celebrity" vulnerability is disclosed to the industry (eg: log4j)
If possible vulnerability management teams scan enterprise networks to identify affected software and/or devices. OT environments normally not scanned left due to segmentation and reliability concerns.	Vulnerability management teams search the Finite State Platform for the specific CVE or software component and a list of identified products is displayed
Contact all software and device vendors via TPRM questionnaire to determine vulnerability applicability, impact, and mitigations	Impacted product vendors are directly contacted to validate exploitability while understanding impact and available mitigations
Exposure and response dependent on vendors response time	Immediate response and mitigation efforts for impacted IT and OT devices occur
Mean time to vulnerability identification and response: Months	**Mean time to vulnerability identification and response: Days**

About Finite State

Finite State enables the teams responsible for the most critical connected infrastructures to protect the devices we rely on every day through market-leading software threat, vulnerability, and risk management.

By analyzing every piece of information in device firmware, from third-party code to configuration settings, Finite State enables secure device manufacturing at scale. Our products and services integrate seamlessly into existing development and SecOps processes and provide actionable security metrics to address product and supply chain risk.

FINITE STATE

finitestate.io