FINITE STATE

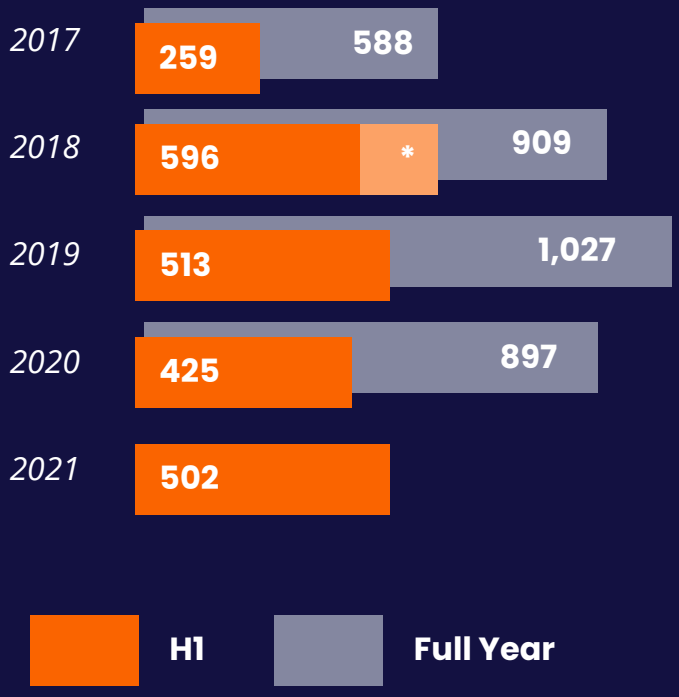
Finite State for Asset Owners

Automated product risk assessment and software supply chain transparency

@FiniteStateInc
/company/FiniteState
www.finitestate.io

Even the most trusted vendors ship vulnerable software

New vulnerabilities in network devices over 5 years



** 2018 was an outlier due to the large number of vulnerabilities reported on Huawei devices in the first half of the year*

*** from Skybox Security: Vulnerability and Threat Trends Mid-Year Report 2021*

Finite State for Asset Owners

Automated product risk assessment and software supply chain transparency

Supply chain risk is critical infrastructure risk.

Seemingly overnight, the proliferation of connected devices has brought device supply chain risk to the forefront and fundamentally changed the nature of risk management in critical infrastructure. Asset owners, who typically don't have the in-house knowledge to manage device supply chain risk, have tried to keep pace, knowing that connected devices expose them to tremendous supply chain risk.

Without access to a purpose-built solution to help manage device supply chain risk, asset owners are resigned to using the fallbacks of manual third-party risk assessments and manual penetration testing. In using third party risk assessments, asset owners are dependent on vendors to provide accurate information, and left with little option but to trust these very device manufacturers who typically operate unaware of the vulnerabilities introduced by their own supply chains. And while penetration testing offers a slightly more accurate view of risk, it too is far from complete. Further, being cost and resource intensive, penetration testing is used sparingly.

The biggest shortcoming may be that even if perfectly accurate, risk assessments and penetration testing are only accurate at a single point in time, and would quickly be rendered obsolete against the backdrop of a dynamic threat landscape – leaving asset owners once again exposed to an ever growing, unknown, unquantified supply chain risk.

Platform at a Glance

Finite State's Platform for Asset Owners was built from the ground up to help tackle this complex problem – managing device supply chain risk. It provides:

- Continuous visibility into connected device supply chain risk.
- Comprehensive SBOMs and cyber risk profile.
- Vendor and asset owner collaboration and verification.
- Live view into risk and vulnerability data.

Already daunting, the complexity and magnitude of managing device supply chain risk only becomes fully understood when considering that this challenge happens at a scale of hundreds of connected devices that a typical asset owner might have on their network.

Shortcomings of traditional risk assessments & pen testing:

- Manual, costly, labor intensive processes.
- Provide incomplete information.
- Doesn't scale to meet the proliferation of connected devices.

The Finite State Platform

Technology

Finite State's unified platform empowers you to effectively manage your supply chain risk, and uses both advanced software composition analysis (SCA) and static application security testing (SAST) to surface even deeply obscured vulnerabilities. This makes the Finite State platform a perfect complement to existing AppSec tools, which lack the capability to analyze connected device firmware and third party components, leaving you blind to critical vulnerabilities latent in device firmware.

Compared to traditional penetration tests, which are limited to point-in-time visibility, not only is Finite State a dramatically lower cost per SKU, it also provides continuous visibility of your supply chain, which is imperative to managing the security of critical infrastructure.

What you get

Automated Vendor Product Security Assessments
Built on the foundation of the industry's largest ground truth database of 350,000+ firmware packages.

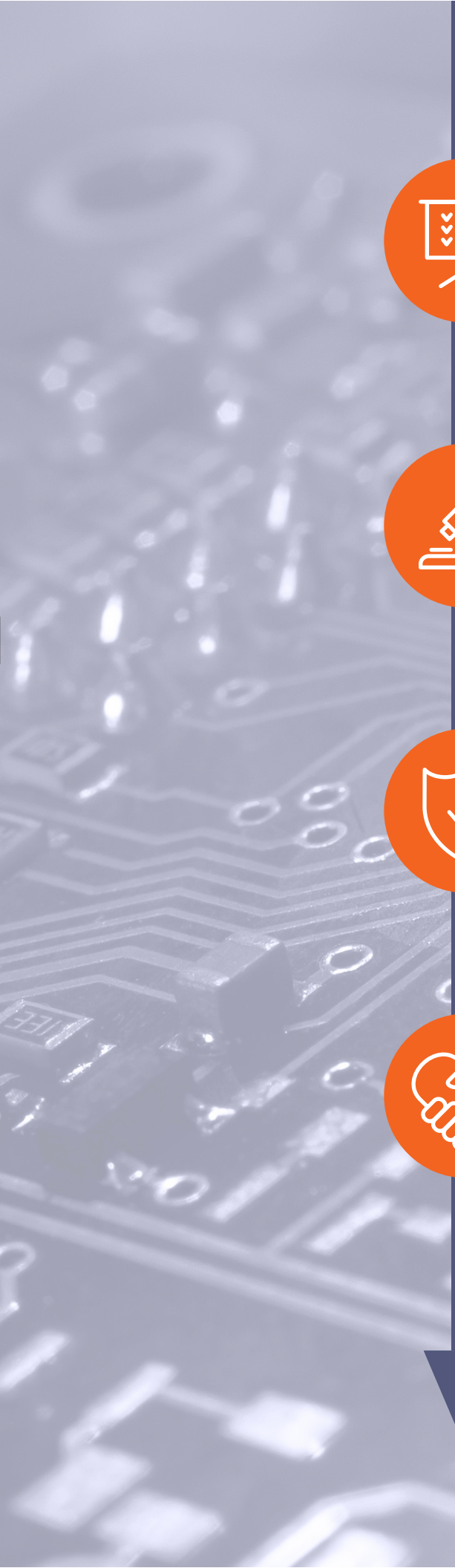
Class-defining Software Composition Analysis
With 11 matching criteria, Finite State's SCA provides the most comprehensive view into SBOM components, limiting exposure to undiscovered vulnerabilities.

Deep SAST Capabilities
The Finite State Platform probes the underlying code within firmware for potential vulnerabilities.

Vendor SBOM Repository
Providing real-time visibility into supply chain vulnerabilities. Optimized to facilitate frictionless vendor firmware acquisition.

Continuous Vulnerability Identification
With real time notifications to enable your team to act quickly when a new CVE is reported.

Vulnerability Analysis Engineer
Expand your team's capability and effectiveness with support to help your organization translate findings into actionable items.



Onboard

Initiate a new product risk assessment. Enable procurement, vendor risk assessment, and cyber security teams to assess the risk of new products being procured or updated on your network.

Assess

Review uploaded product risk data including: SBOM, HBOM, Vendors in Supply Chain, Static Analysis Results, SDLC approach, Pen Test Results, Privacy Data, Certifications and Standards.

Simplify analysis through Finite State risk ratings and benchmarks.

Verify

Leverage the platform's automated binary analysis capabilities to verify the security of the software and go beyond vendor-provided results.

Verify the authenticity and integrity of software packages prior to deployment by comparing to verified artifacts.

Collaborate

With an established connection with your vendor's product security team, enable secure communication and collaboration.

Report discovered vulnerabilities and threats instantly.

Work with your vendors to verify the availability and security of patches.

People & Process

With the Finite State Security Research & Support team behind you every step of the process, even time-strapped security teams punch above their weight. Your team will have the peace of mind that supply chain risk is monitored and mitigated on a continuous basis, and connected devices are safe to deploy across your network.

Finding and retaining highly skilled cybersecurity staff continues to be a major pain point for asset owners across the country. With the growing global concern around supply chain security, Asset Owners need to quickly build and mature their vendor risk assessment process and product procurement program and demand more visibility into their device supply chains to fend off attacks such as SolarWinds and Log4J.

Running a successful supply chain security program requires people with expert knowledge in reverse engineering binaries and organizational process development. We understand these types of resources aren't easy to hire or retain, which is why the Finite State Platform for Asset Owners supports you with the following expertise to ensure your program's success:

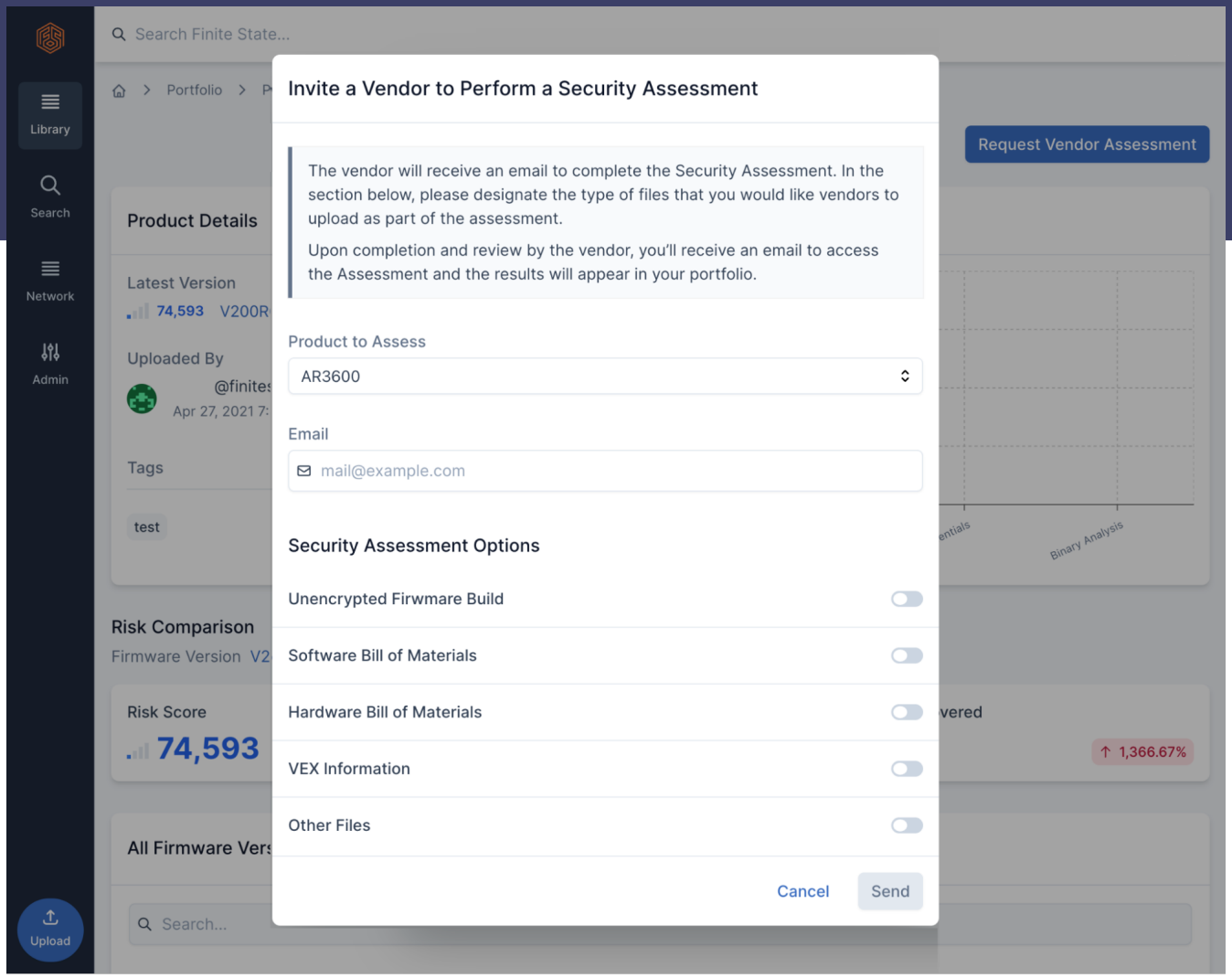
Supply Chain Risk Manager

- Provides proven program template to reduce supply chain risk
- Helps establish product and vendor risk assessment into existing procurement process
- Works with OEMs to gather information:
  - » Firmware images
  - » Hardware information
  - » Provenance information
  - » Mitigation, patch, and firmware update details
- Organizes monthly operational meetings, action plans, and quarterly executive reviews

Firmware Vulnerability Analyst

- Reviews and interprets results of binary analysis (highlights top 3-5 items per analysis)
- Verifies applicability and/or exploitability of any issues (if required)
- Prioritizes security issues for either asset owner and/or vendors
- Provides custom remediation guidance to developers
- Owns impact assessment for critical or high profile issues
- Helps to identify compliance violations

Collaborative Risk Assessments



- *Customizable requests for security data*
- *Collect robust security data including SBOM, VEX, HBOM, SAST results, SDLC data, etc.*
- *Collaborate on identified issues and remediations*
- *Full audit trail*
- *Issue tracking*

Why you should work with Finite State:

Finite State's industry leading binary analysis platform has been built by experts with over two decades of firmware reverse engineering for both offensive and defensive research purposes. The platform is considered the most advanced on the market today because of the patented methods and algorithms used to identify and match software subcomponents within proprietary embedded devices while also highlighting hardcoded credentials, known vulnerabilities (CVEs), zero-day vulnerabilities (MITRE CWEs), and critical misconfigurations of apps and services.

Mature your vendor risk assessments

Leverage ground truth data and generate a repository of the components found within connected devices in your inventory.

Lessen vulnerability impact

Shorten vulnerability impact, scoping, and response times by pinpointing the origin and scope of risk using a live inventory of the device components within your organization.

Scale your device pen tests

Reduce time and costs to test your devices by leverageing Finite State's automated firmware analysis across your device inventory.

Free your team to focus

Take advantage of our world class vendor firmware security researchers and support teams to ensure your success. Enable your team to work on the issues they best know how to solve.