The Finite State Next Generation Platform

Comprehensive Software Risk Management for the Connected World

FINITE STATE

OVERVIEW

The Finite State Next Generation platform provides product security teams and artifact owners a comprehensive view of their risk profile at every link in the software supply chain. Built on a strong foundation of best-in-class firmware binary analysis, the Next Generation platform unifies data from over 120 vulnerability scanners on the market, correlating the analysis and distilling it into an intuitive risk score and easy-to-read remediation guidance for the most seamless supply chain risk management experience on the market.

Connected devices comprise society's invisible engine, powering operations in the world's most critical industries, like energy, automotive manufacturing, and medical technology. The complexity of connected device security, especially in highly industrialized verticals like these, makes it impossible to ensure a complete understanding of risk, let alone take action on all of the vulnerabilities.

This leads to numerous issues, like:

- Vulnerabilities going unaddressed, either unidentified or underestimated
- Vulnerabilities becoming exploits and then breaches, costing significant outlays of money and time — and eroding trust
- Fines for non-compliance with regulatory requirements
- Derailed resource and growth plans as the business is forced to react

Where the Next Gen Platform Comes In

The Next Gen platform manages this complexity, arming the teams responsible for product and artifact security with the key intelligence they need to take action on vulnerabilities and manage the risks in their supply chain at every level, from the firmware up.

The Next Gen platform looks both wide and deep for vulnerabilities — correlating risk data across a breadth of scanning tools, and breaking down the risk level and remediation guidance from the product view all the way down to each individual artifact.

Get the key intelligence needed to take action on vulnerabilities and manage the risks at every level of your supply chain— from the firmware up.

Key Capabilities

- Our platform provides a comprehensive view for Product Security teams to organize and learn from the mountain of data available to them
- Shift security testing to the right of the build cycle with flagship firmware binary analysis; make vulnerability and risk management a part of your operational cadence
- Gain unprecedented visibility with firmware binary analysis and vulnerability correlation with over 120 third-party scanners
- Prioritize remediation efforts without the headaches, using rigorously defined risk scores and dead-simple remediation guidance on every product and artifact
- Satisfy regulatory compliance requirements with thorough Bill of Materials generation for deeper component documentation in software, hardware, and production BOMs

Our Differentiators

Firmware Binary Composition Analysis

Within the landscape of products providing software composition analysis, we have established ourselves as a leader through our focus on firmware binaries. Our proprietary technology enables the owners and makers of connected devices to understand every component in the supply chain and its level of risk, down to the metal.

Vulnerability Management

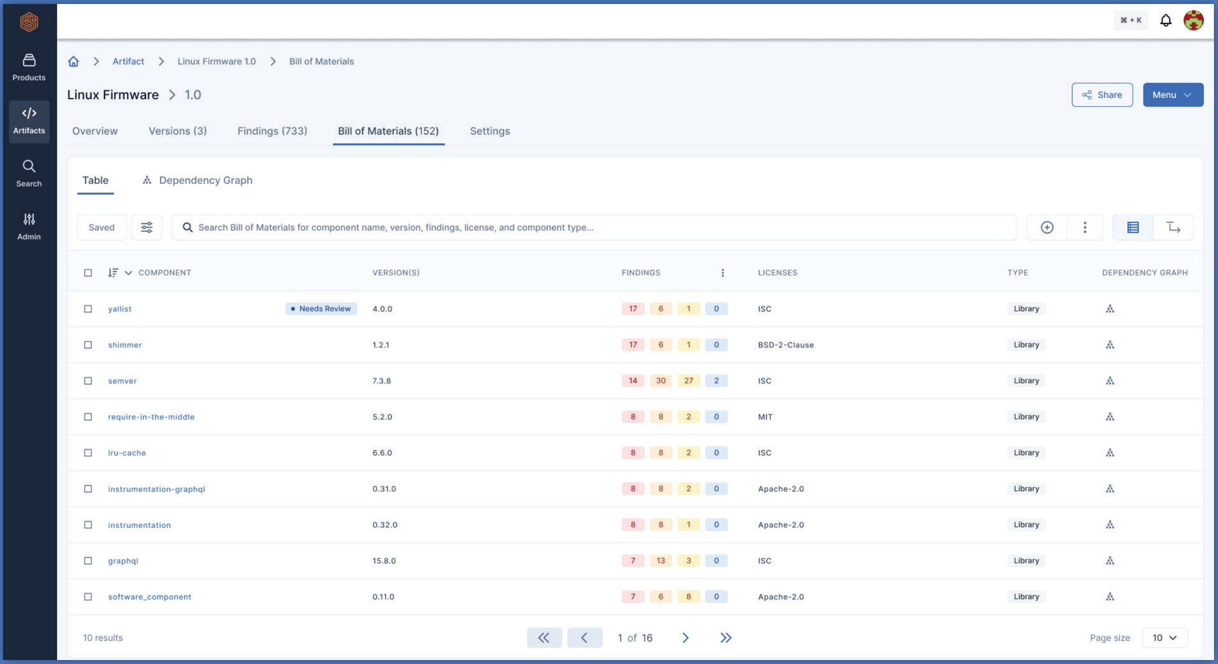
We are the only product on the market that, along with our leading binary SCA capability, offers the ability to load in scans from over 120 scanners, creating a comprehensive risk profile — synthesized into an intuitive score — that empowers teams to prioritize and act on vulnerabilities quickly, building resilience and stewardship into their security operations.

Software Bill of Materials

With our unparalleled visibility into the components and vulnerabilities at every link in the supply chain, now complemented by the ability to upload scans from scores of other providers, we are equipped to produce the most thorough, detailed Bill of Materials documentation for all of your assets, enabling easy compliance with regulatory frameworks for cybersecurity.

White-Glove Service and Support

We are a leading software supply chain security company, a collective of security experts, and a group of folks who have been in your shoes, working to manage supply chain risk with inadequate tools and information overload. We are here to bring that experience to bear to support you whenever needed. You're never on your own.



□	COMPONENT		VERSION(S)	FINDINGS				LICENSES	TYPE	DEPENDENCY GRAPH
□	yallist	● Needs Review	4.0.0	17	6	1	0	ISC	Library	⁂
□	shimmer		1.2.1	17	6	1	0	BSD-2-Clause	Library	⁂
□	semver		7.3.8	14	30	27	2	ISC	Library	⁂
□	require-in-the-middle		5.2.0	8	8	2	0	MIT	Library	⁂
□	lru-cache		6.6.0	8	8	2	0	ISC	Library	⁂
□	instrumentation-graphql		0.31.0	8	8	2	0	Apache-2.0	Library	⁂
□	instrumentation		0.32.0	8	8	1	0	Apache-2.0	Library	⁂
□	graphql		15.8.0	7	13	3	0	ISC	Library	⁂
□	software_component		0.11.0	7	6	8	0	Apache-2.0	Library	⁂

10 results

1 of 16

Page size 10

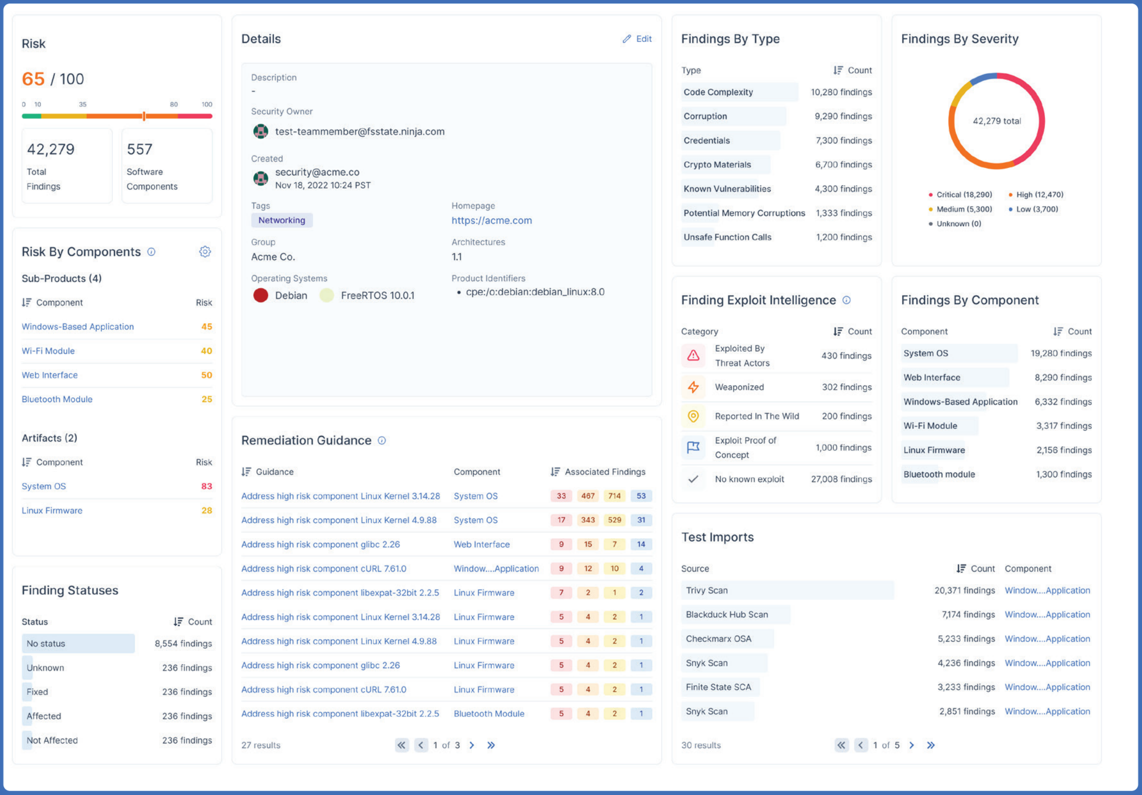
An end-to-end SBOM solution, Finite State is the most comprehensive solution for generating, collecting, visualizing, and distributing SBOMs in your supply chain

Key Features

World-class Binary Software Composition Analysis

Enhanced SBOM capabilities help you decompose products or assets into their many components for a laser-focused risk assessment.

Our Next Generation platform addresses the needs of software producers and consumers to drive down software supply chain risk with the peace of mind they need to ship or deploy connected products securely.



Risk

65 / 100

42,279 Total Findings

557 Software Components

Risk By Components

Sub-Products (4)

Component	Risk
Windows-Based Application	45
Wi-Fi Module	40
Web Interface	50
Bluetooth Module	25

Artifacts (2)

Component	Risk
System OS	83
Linux Firmware	28

Finding Statuses

Status	Count
No status	8,554 findings
Unknown	236 findings
Fixed	236 findings
Affected	236 findings
Not Affected	236 findings

Details

Description: -

Security Owner: test-teammember@fsstate.ninja.com

Created: security@acme.co Nov 18, 2022 10:24 PST

Tags: Networking

Homepage: https://acme.com

Group: Acme Co.

Architectures: 1.1

Operating Systems: Debian FreeRTOS 10.0.1

Product Identifiers:
- cpe:/o:debian:debian_linux:8.0

Remediation Guidance

Guidance	Component	Associated Findings			
Address high risk component Linux Kernel 3.14.28	System OS	33	467	714	53
Address high risk component Linux Kernel 4.9.88	System OS	17	343	529	31
Address high risk component glibc 2.26	Web Interface	9	15	7	14
Address high risk component cURL 7.61.0	Window....Application	9	12	10	4
Address high risk component libexpat-32bit 2.2.5	Linux Firmware	7	2	1	2
Address high risk component Linux Kernel 3.14.28	Linux Firmware	5	4	2	1
Address high risk component Linux Kernel 4.9.88	Linux Firmware	5	4	2	1
Address high risk component glibc 2.26	Linux Firmware	5	4	2	1
Address high risk component cURL 7.61.0	Linux Firmware	5	4	2	1
Address high risk component libexpat-32bit 2.2.5	Bluetooth Module	5	4	2	1

27 results 1 of 3

Findings By Type

Type	Count
Code Complexity	10,280 findings
Corruption	9,290 findings
Credentials	7,300 findings
Crypto Materials	6,700 findings
Known Vulnerabilities	4,300 findings
Potential Memory Corruptions	1,333 findings
Unsafe Function Calls	1,200 findings

Findings By Severity

Finding Exploit Intelligence

Category	Count
Exploited By Threat Actors	430 findings
Weaponized	302 findings
Reported In The Wild	200 findings
Exploit Proof of Concept	1,000 findings
No known exploit	27,008 findings

Findings By Component

Component	Count
System OS	19,280 findings
Web Interface	8,290 findings
Windows-Based Application	6,332 findings
Wi-Fi Module	3,317 findings
Linux Firmware	2,156 findings
Bluetooth module	1,300 findings

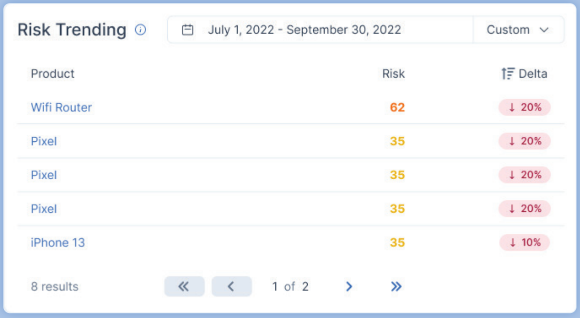
Test Imports

Source	Count	Component
Trivy Scan	20,371 findings	Window....Application
Blackduck Hub Scan	7,174 findings	Window....Application
Checkmarx OSA	5,233 findings	Window....Application
Snyk Scan	4,236 findings	Window....Application
Finite State SCA	3,233 findings	Window....Application
Snyk Scan	2,851 findings	Window....Application

30 results 1 of 5

Intuitive Risk Score That Takes All Data into Account and Reflects Trend Over Time

Finite State's Next Generation Platform delivers an intituve, robust scoring system that conveys risk levels of products and assets at any point in time and over time through a straightforward numerical scale, backed by sophisicated risk prioritization.



Risk Trending

July 1, 2022 - September 30, 2022

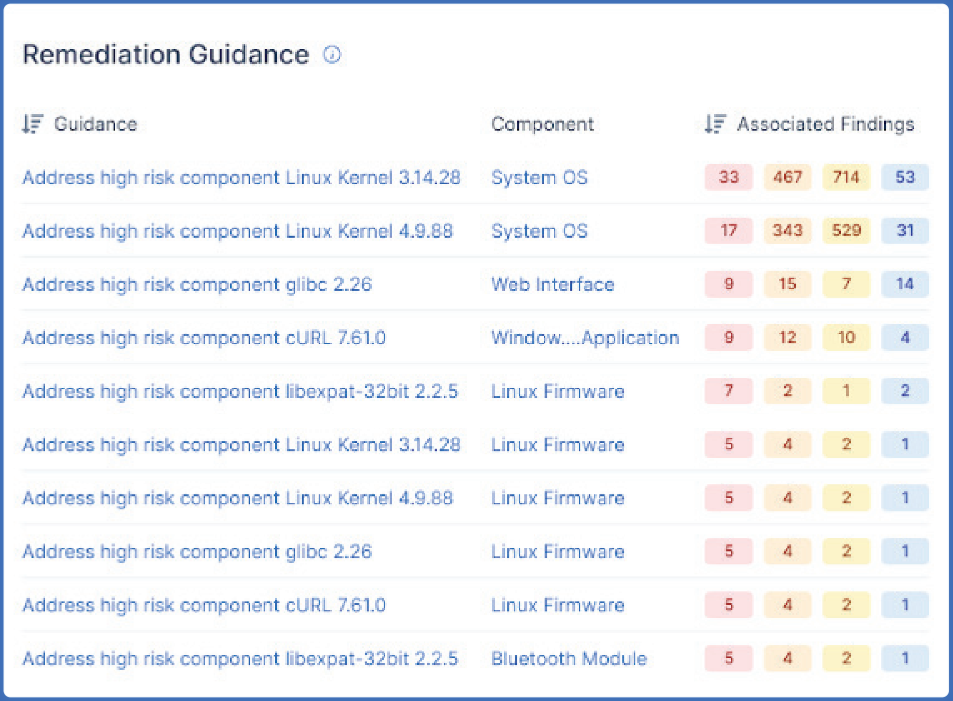
Product	Risk	Delta
Wifi Router	62	↓ 20%
Pixel	35	↓ 20%
Pixel	35	↓ 20%
Pixel	35	↓ 20%
iPhone 13	35	↓ 10%

8 results 1 of 2

KEY FEATURES CONTINUED

Remediation Guidance to Support Decisive Action

The Next Generation Platform delivers advanced remediation guidance that aggregates and reconciles results across all scans, generated or ingested, for context-aware recommendations.

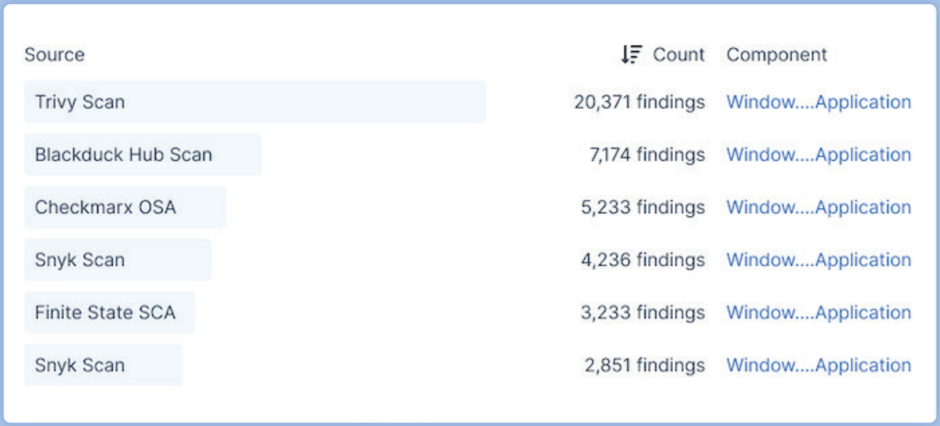


Remediation Guidance

Guidance	Component	Associated Findings			
Address high risk component Linux Kernel 3.14.28	System OS	33	467	714	53
Address high risk component Linux Kernel 4.9.88	System OS	17	343	529	31
Address high risk component glibc 2.26	Web Interface	9	15	7	14
Address high risk component cURL 7.61.0	Window....Application	9	12	10	4
Address high risk component libexpat-32bit 2.2.5	Linux Firmware	7	2	1	2
Address high risk component Linux Kernel 3.14.28	Linux Firmware	5	4	2	1
Address high risk component Linux Kernel 4.9.88	Linux Firmware	5	4	2	1
Address high risk component glibc 2.26	Linux Firmware	5	4	2	1
Address high risk component cURL 7.61.0	Linux Firmware	5	4	2	1
Address high risk component libexpat-32bit 2.2.5	Bluetooth Module	5	4	2	1

Rigorous Correlation and Analysis with Third-party Scan Uploads

Ingesting data from over 120 scanners and feeds, the Next Generation platform unifies all of your tooling and intelligence to help you secure your products and systems, within the full context of your AppSec or Product Security environment.



Source	Count	Component
Trivy Scan	20,371 findings	Window....Application
Blackduck Hub Scan	7,174 findings	Window....Application
Checkmarx OSA	5,233 findings	Window....Application
Snyk Scan	4,236 findings	Window....Application
Finite State SCA	3,233 findings	Window....Application
Snyk Scan	2,851 findings	Window....Application

Pricing

The Next Gen platform is priced to allow flexibility and correspond closely with the value we provide to each business. We offer several plan levels that, for a flat annual fee, allow use of features relevant to the business, with unlimited document uploads and integrations and no per-seat limits. Ensure all the important team members in your security team can do their jobs with no extra investment.

We also offer a number of add-ons that can be purchased a la carte. This gives us the building blocks we need to create a just-right package for every business.

For more information about our pricing, please contact us.

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