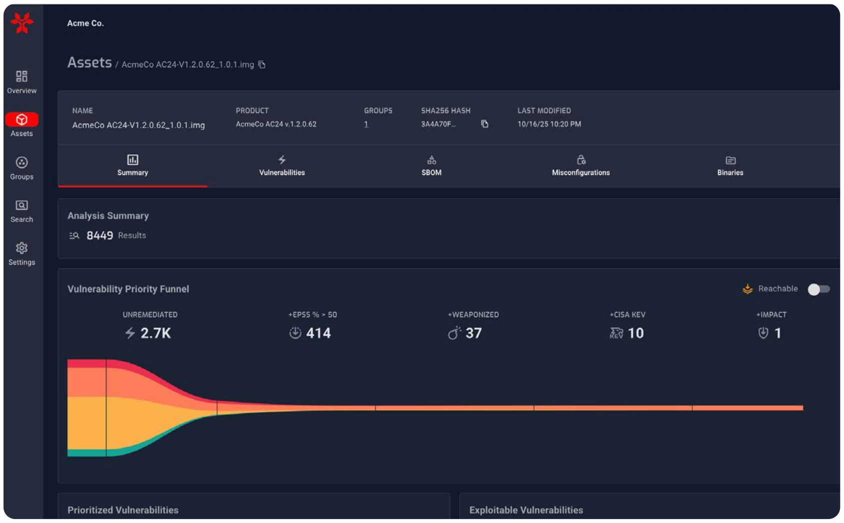
NETRISE

Data Sheet

What's Inside *Your* Software?

Protect your financial services institution from Software Supply Chain Security risk by analyzing compiled code rather than source code.

NetRise provides deep visibility into compiled software across networking and security devices, core banking platforms, trading systems, ATMs, and fintech—so institutions can proactively identify and manage supply chain risk threatening operational resilience and regulatory compliance.



Acme Co.

Assets / AcmeCo AC24-V1.2.0.62_1.0.1.img

NAME	PRODUCT	GROUPS	SHA256 HASH	LAST MODIFIED
AcmeCo AC24-V1.2.0.62_1.0.1.img	AcmeCo AC24 v.1.2.0.62	1	3A4A70F...	10/16/25 10:20 PM

Analysis Summary

8449 Results

Vulnerability Priority Funnel

UNREMEDIATED	+EPSS % > 50	+WEAPONIZED	+CISA KEV	+IMPACT
2.7K	414	37	10	1

Prioritized Vulnerabilities

Exploitable Vulnerabilities

Why NetRise Is Different

NetRise assesses the results of a software build, identifying all of the components in the binary image, and finding risk beyond CVEs and CWEs. Our platform tells you which vulnerable code runs at startup, so you can prioritize risk reduction.

- **No Source Code Required:** Rather than rely on vendor self-assessments, verify what runs in the code on devices and in apps you've bought.
- **Beyond CVEs:** There's more to risk than CVEs. We identify misconfigurations, hard-coded secrets, public and private keys, and more.
- **Exploitability Insight**: It's easy to be overwhelmed by vulnerability findings. NetRise tells you what is reachable at runtime, so that you can prioritize action.
- **Integrations:** NetRise integrates into your workflows and into other tools used in your SOC.

Who Uses NetRise?

CISOs & CROs

Gain continuous insight into the software supply chain of critical banking and trading applications built internally, enterprise third-party risk management, and regulatory reporting.

GRC and Compliance Teams

Automatically generate binary-derived SBOM-driven evidence for audits aligned with PCI DSS 4.0, NYDFS, SEC Cybersecurity Rules, FFIEC, and NAIC Model Law—reducing manual reporting and enhancing regulator confidence.

Third-Party Risk & Vendor Management Teams

Assess, with no source code required, the security posture of networking and security devices, fintech platforms, SaaS solutions, and any software purchased by your institution.

Security Operations Teams

Identify affected systems and triage vulnerabilities in network devices using exploitability context.

Mobile and Web App Developers

Find and fix post-build risks before release, validate SBOMs, and prioritize patches faster.

Tailored Solutions for Your Institution

For Those Who Buy, Use, and Maintain Software

(Mobile and Web App Developers, Third-Party Risk, Compliance)

- Know what's really executing in your environment.
- Build and maintain a comprehensive software asset inventory.
- Verify risk associated with networking, security, and third-party devices and software you procure, rather than relying on vendor self-attestation.
- Uncover hidden risk beyond code, such as hard-coded secrets, misconfigurations, and public and private keys, which can provide root access across your network.
- Prioritize mitigation based on reachability findings.
- Demonstrate compliance with regulatory frameworks.
- Validate that builds match declared manifests and intended components, ensuring no unexpected code is introduced.
- Gain visibility into legacy software components used in core banking platforms, where source code may be unavailable.
- Rapidly assess the software supply chain of M&A targets or third-party fintech integrations.

Features

Binary Composition Analysis

Uncover secrets, misconfigurations, and public and private keys from networking, security, and device firmware, as well as compiled software components.

SBOM Management

Generate, enrich, and validate SBOMs for networking and security devices, third-party software, and internally built applications—providing full transparency across all components.

NetRise ZeroLens™

Detect exploitable weaknesses in vendor or internal software early, before they affect production systems.

NetRise Trace™

AI-powered intent-driven search, based on the underlying motives behind the code.

Kernel Vulnerability Auto-Remediation

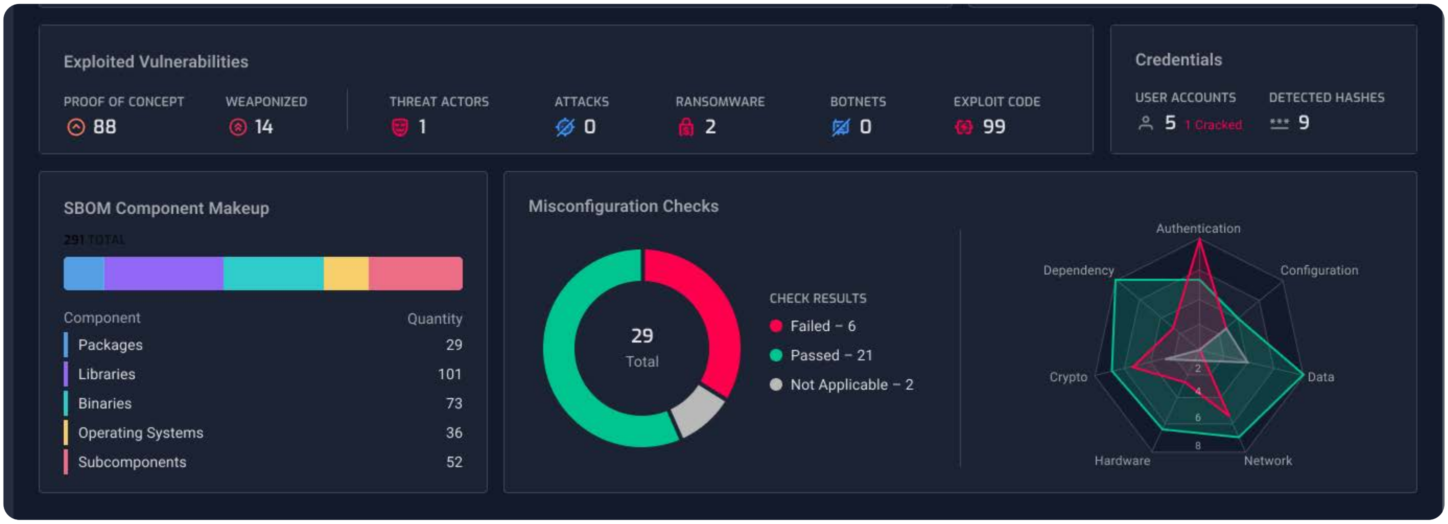
Eliminate kernel vulnerability noise with automated validation and VEX-compliant evidence, so teams focus on exploitable issues, not false positives.

Vulnerability Intelligence

Gain deeper context into findings, identifying and prioritizing those that have been weaponized and exploited.

Ensuring Compliance

Produce audit-ready evidence aligned with, PCI DSS 4.0, NYDFS, SEC, NAIC, GDPR/CCPA, and supporting frameworks like EO 14028, DORA, and the EU CRA.



Exploited Vulnerabilities

PROOF OF CONCEPT	WEAPONIZED	THREAT ACTORS	ATTACKS	RANSOMWARE	BOTNETS	EXPLOIT CODE
88	14	1	0	2	0	99

Credentials

USER ACCOUNTS	DETECTED HASHES
5 1 Cracked	9

SBOM Component Makeup

291 TOTAL

Component	Quantity
Packages	29
Libraries	101
Binaries	73
Operating Systems	36
Subcomponents	52

Misconfiguration Checks

29 Total

CHECK RESULTS

- ● Failed – 6
- ● Passed – 21
- ● Not Applicable – 2

Deploy with Ease

NetRise integrates with the workflow and reporting tools your teams already use, streamlining device security assessments and compliance processes.

Start Scanning in Minutes

Get visibility into software assets almost immediately.

API-First Design

Integrate into build pipelines, CMDBs, and risk systems.

Cloud-Native

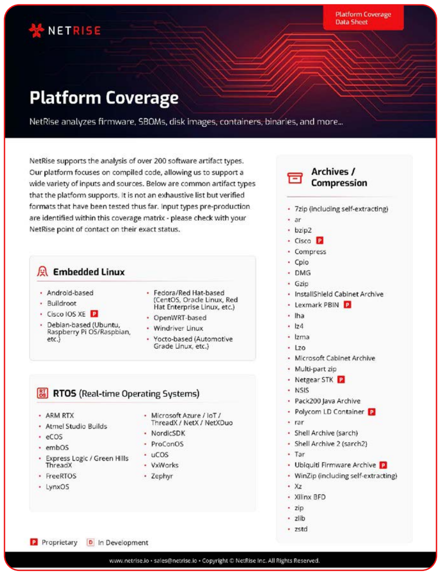
Scale easily without infrastructure overhead.

Broad OS Support

Analyze Linux, Windows, and RTOS.

Explore Platform Coverage

The NetRise Platform Coverage Sheet provides a detailed look at supported binaries, firmware formats, OS targets, and embedded components—so you know exactly what NetRise can analyze.



NETRISE

Platform Coverage Data Sheet

Platform Coverage

NetRise analyzes firmware, SBOMs, disk images, containers, binaries, and more...

NetRise supports the analysis of over 200 software artifact types. Our platform focuses on compiled code, allowing us to support a wide variety of inputs and sources. Below are common artifact types that the platform supports. It is not an exhaustive list but verified formats that have been tested thus far. Input types pre-production are identified within this coverage matrix - please check with your NetRise point of contact on their exact status.

Embedded Linux

- Android-based
- Buildroot
- Cisco IOS XE P
- Debian-based (Ubuntu, Raspberry Pi OS/Raspbian, etc.)
- Fedora/Red Hat-based (CentOS, Oracle Linux, Red Hat Enterprise Linux, etc.)
- OpenWRT-based
- Windriver Linux
- Yocto-based (Automotive Grade Linux, etc.)

RTOS (Real-time Operating Systems)

- ARM RTX
- Atmel Studio Builds
- eCOS
- embOS
- Express Logic / Green Hills ThreadX
- FreeRTOS
- LynxOS
- Microsoft Azure / IoT / ThreadX / NetX / NetXDuo
- NordicSDK
- ProConOS
- uCOS
- VxWorks
- Zephyr

Archives / Compression

- 7zip (including self-extracting)
- ar
- bzip2
- Cisco P
- Compress
- Cpio
- DMG
- Gzip
- InstallShield Cabinet Archive
- Lexmark PBIN P
- lha
- lz4
- lzma
- Lzo
- Microsoft Cabinet Archive
- Multi-part zip
- Netgear STK P
- NSIS
- Pack200 Java Archive
- Polycom LD Container P
- rar
- Shell Archive (sarch)
- Shell Archive 2 (sarch2)
- Tar
- Ubiquiti Firmware Archive P
- WinZip (including self-extracting)
- Xz
- Xilinx BFD
- zip
- zlib
- zstd

P Proprietary D In Development

www.netrise.io • sales@netrise.io • Copyright © NetRise Inc. All Rights Reserved.

What's Inside *Your* Software?

Let's Find Out