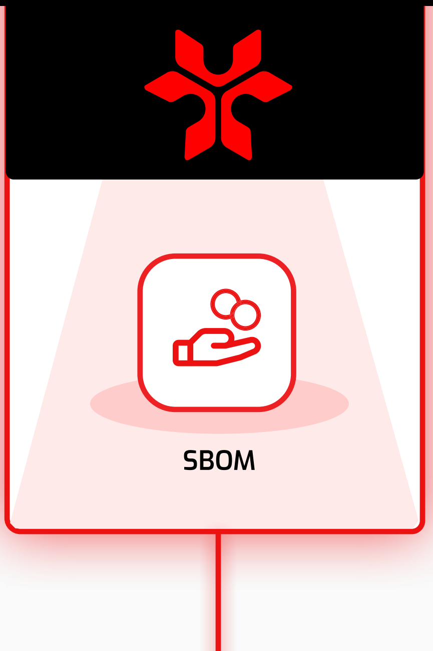
Enterprise Solution Brief

NETRISE

What's Inside *Your* Software?

Gain visibility into the software that runs the hardware you purchase with NetRise.

Manage risk in the software your organization buys, uses, and operates.



THE CHALLENGE

You’re Purchasing Devices to Run on Your Network. How Do You Vet Them?

SBOM

Ask yourself a few basic questions:

- Do you know whether Log4j still executes anywhere across your enterprise systems?
- Can you say how many versions of OpenSSL are active in production, test, or unmanaged environments?
- Do you know which components that autorun at startup contain exploitable vulnerabilities?

If you’re not sure, you’re not alone. Most organizations today rely on opaque software systems that legacy application security solutions can’t see.

- Legacy AppSec tools focus on source code, but most software your business relies on is vendor-supplied, and source code often isn’t available.
- Vendor-supplied SBOMs, often inaccurate due to undocumented builds and shifting dependencies, expose you to additional risk.
- Critical risk lives outside the source code —in containers, misconfigurations, credentials, and hidden scripts.

You wouldn’t tolerate that level of unknown risk in your hardware inventory. Why accept it for your software?

SOFTWARE ASSET INVENTORY

Where Verification Starts, And Security Follows

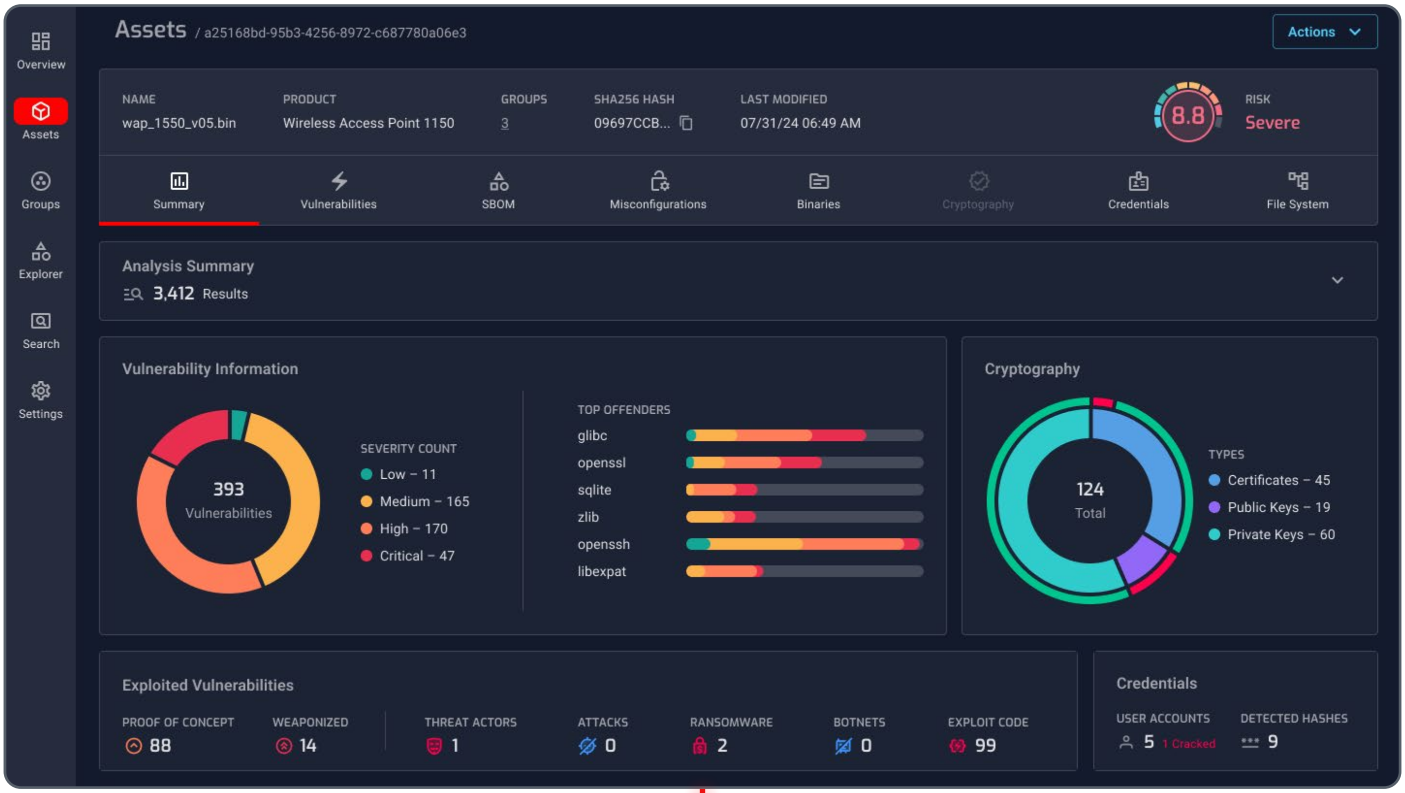
Enterprise software includes proprietary and third-party code, libraries, dependencies, operating systems, firmware, containers, configuration files, credentials, scripts, virtual machines, and the packages that manage them.

To manage risk, you need visibility into the compiled software that actually executes in your environment.

THE SOLUTION

NetRise for Those Who Buy, Use, and Maintain Software

NetRise is redefining software supply chain security. By analyzing compiled code—firmware, packages, and device-level software—NetRise creates comprehensive and accurate software inventories that expose hidden risk and improve security posture.



Assets / a25168bd-95b3-4256-8972-c687780a06e3

NAME	PRODUCT	GROUPS	SHA256 HASH	LAST MODIFIED	RISK
wap_1550_v05.bin	Wireless Access Point 1150	3	09697CCB...	07/31/24 06:49 AM	8.8 Severe

Analysis Summary
3,412 Results

Vulnerability Information

393 Vulnerabilities

SEVERITY COUNT
- Low – 11
- Medium – 165
- High – 170
- Critical – 47

TOP OFFENDERS
- glibc
- openssl
- sqlite
- zlib
- openssh
- libexpat

Cryptography

124 Total

TYPES
- Certificates – 45
- Public Keys – 19
- Private Keys – 60

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

NetRise: A System of Intelligence for Enterprise Software Security

Whether you manage endpoints, deploy third-party software, or oversee critical infrastructure, NetRise helps you:

See what's actually in your software

Validate your Software Bill of Materials (SBOM) with a binary-derived inventory of the code that actually executes.

Make smarter purchasing decisions

Use verified software inventory to assess supplier risk, compare products, and drive remediation through procurement.

Analyze third-party code without waiting

Inspect inbound software and devices without relying on vendor self-attestations or delayed disclosures.

Track exposure across your environment

Search for vulnerable components across all systems, software, and suppliers, at speed and scale.

Support audits. Secure procurement workflows

Generate reports mapped to requirements like Executive Order 14028, E.U. CRA, NIST guidance, and public-sector security mandates.

Platform Overview

Software Asset Inventory and Transparency

Build complete, binary-derived Software Bills of Materials (SBOMs) that reflect what's truly in your software, not just what's declared. Capture additional artifacts such as misconfigurations, credentials, certificates, and scripts.

Binary Composition Analysis

Analyze compiled third-party and proprietary software—no source access required. Understand what's actually executing in your environment across firmware, containers, and packaged applications.

System of Intelligence for Software Risk

Enrich your software inventory with vulnerability context, Common Weakness Enumerations (CWEs), exploitability, reachability, and licensing indicators to prioritize and manage risk effectively.

Compliance Without Bottlenecks

Generate audit-ready reports aligned to Executive Order 14028, the EU Cyber Resilience Act (CRA), ISO 27001, and NIST CSF 2.0—without slowing procurement, onboarding, or operations.

NetRise delivers the visibility and context organizations need to reduce real-world software risk.

Why NetRise Stands Apart

Exploit-Aware Prioritization

Focus on real risk with enriched vulnerabilities including weaponization, privileges, and CVSS impact.

Reachability Insights

Identify components that autorun or initialize at startup to prioritize fixes in high-risk code.

Seamless Integrations

Automate workflows across ticketing, compliance, SIEM, and asset management via robust APIs.

ZeroLens

Detect weaknesses and CWEs in compiled software before they're assigned CVEs. Get a head start on remediation.

Trace

Understand software provenance, validate vendor claims, and track unauthorized changes using AI-powered search.

Key Use Cases

Threat Response and Mitigation

Locate, prioritize, and remediate risk fast when new vulnerabilities emerge.

Procurement Security

Make smarter buying decisions, based on facts, not checklists.

Third-Party and Vendor Risk

Go beyond SBOMs to see executes, no source code required.

Patch Governance

See how updates add risk via functions, dependencies, or vulnerabilities.

Software Asset Inventory

Establish real-time code-based visibility aligned with CIS Control #2.

With NetRise, you move from software uncertainty to software control.

Ready to see what actually executes in your environment?

Let's Find Out