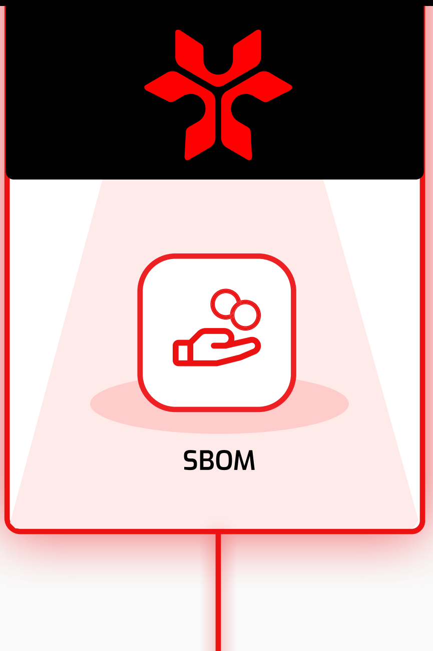
Financial Services
Development Solution Brief

NETRISE

Your Executable Code Hides Risk You Can’t See

Protect your brand, customer trust, and regulatory standing by verifying that the executable code in your financial products matches what’s documented in your Software Bill of Materials (SBOM).

Illuminate hidden risk in compiled software powering your web and mobile apps, trading platforms, and fintech infrastructure—exposing components and vulnerabilities that traditional SBOMs miss.



THE CHALLENGE

Your SBOM Doesn’t Tell the Whole Story

You use the latest application security testing products, and they help your developers write secure code. But vulnerable components that aren’t visible in SBOMs or testing tools can be included in your compiled code. Without binary composition analysis, this risk remains invisible.

- ? Do the component versions in the software build actually match those in your manifest?
- ? Have you unintentionally introduced risk through misconfigurations, hard-coded secrets, or public/private keys not seen by AST tools?
- ? Can you demonstrate to regulators and financial customers exactly what’s inside the systems you provide to your customers?

These gaps persist because:

- Static testing and SCA don’t always reflect what’s actually compiled and built.
- Build processes often introduce old versions of components hidden from SBOMs derived from source code.
- ⚠ Legacy tools ignore risk in configuration files, credentials, scripts, and containers.

For financial services institutions, these blind spots create operational risk and regulatory exposure.

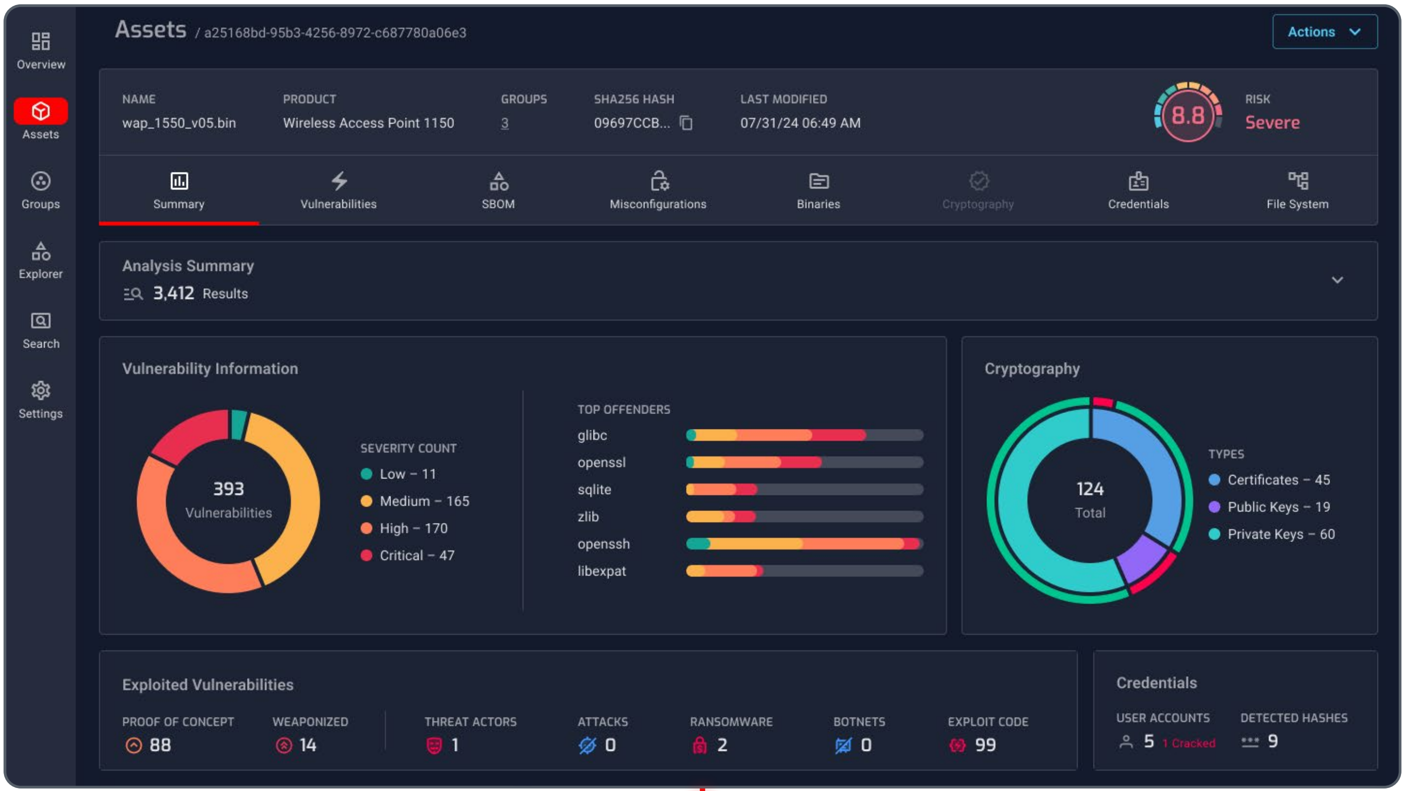
Why You Need a Comprehensive SBOM

Software today is more assembled than written. Research shows that as much as 80% of today's software is derived from third-party components. A single application can include proprietary code, open-source libraries, config files, operating systems, credentials, and more.

THE SOLUTION

NetRise: Software Supply Chain Security for Financial Services Institutions

NetRise gives financial services institutions complete visibility into the software you rely on—across devices, applications, and vendors—so you can uncover hidden risk, strengthen regulatory defensibility, and make faster, more informed security decisions. Unlike legacy tools limited to source-code analysis, NetRise analyzes the software that actually executes in your environment, providing the clarity needed to prioritize action and reduce exposure.



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	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 Finanical Software Security

Whether you build software for financial devices (ATMs, payment terminals), trading appliances, core banking modules, or customer-facing webapps and mobile apps, NetRise helps your teams:

Build with confidence using accurate SBOMs

Generate comprehensive, binary-derived SBOMs to validate what's actually executing in your software, including the origin and integrity of third-party libraries.

Catch build-time deviations

Verify that builds match declared manifests and signed artifacts to ensure software integrity and supply-chain trust.

Prioritize remediation

Ensure updates don't introduce vulnerabilities. Validate kernel CVEs with Kernel Vulnerability Auto-Remediation and prioritize remediation using reachability.

Platform Overview

Software Composition Transparency

Complete binary-derived SBOM offering a comprehensive view of your software supply chain, including source code and other artifacts: misconfigurations, containers, credentials, keys, scripts, and more. Built for regulated financial systems.

Software System of Intelligence

Leverage enriched context around software vulnerabilities—including a description, a reference to the CVE source, advisories, severity metrics, and more—plus exploitability, reachability, and weaponization status to prioritize real risk in financial environments.

Binary Composition Analysis

Analyze compiled and interpreted software to understand component-level relationships and identify hidden software risk.

Compliance Readiness

Deliver audit-ready evidence for key financial and cybersecurity regulations—without slowing development.

NetRise delivers the visibility and context needed to build, certify, and ship secure financial software and devices.

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 remediation.

Kernel Vulnerability Auto-Remediation

Eliminate kernel vulnerability noise with automated validation and VEX-compliant evidence so teams can focus on exploitable issues and simplify audits.

NetRise ZeroLens®

Detect CWEs and risky code patterns in compiled software before they become known vulnerabilities.

Common Challenges Financial Services Institution Developers Face

Challenge	How NetRise Helps
You struggle to prioritize security findings.	**Focus** on vulnerabilities that are weaponized, exploitable, accessible via the network, and that autorun at startup.
You lack visibility into what's in your compiled builds.	**Analyze** compiled binaries and produce comprehensive and accurate SBOMs.
You can't easily see into open-source dependencies.	**Discover** deeper dependencies than are visible through source or SCA scans.
You need audit-ready documentation.	**Provide** clear, regulator-friendly reports to support compliance with financial cybersecurity regulations.

What's inside *your* software? Build trust and meet customer and regulatory expectations with NetRise.

Get Started