NETRISE

What's Inside *Your* Software?

Gain visibility into the software running on networking and security devices, trading platforms, and fintech infrastructure.

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

SBOM

THE CHALLENGE

Your SBOM Doesn't Tell the Whole Story

You're relying on third-party software, networking, and security devices across core banking, payments, and trading systems. How do you vet them?
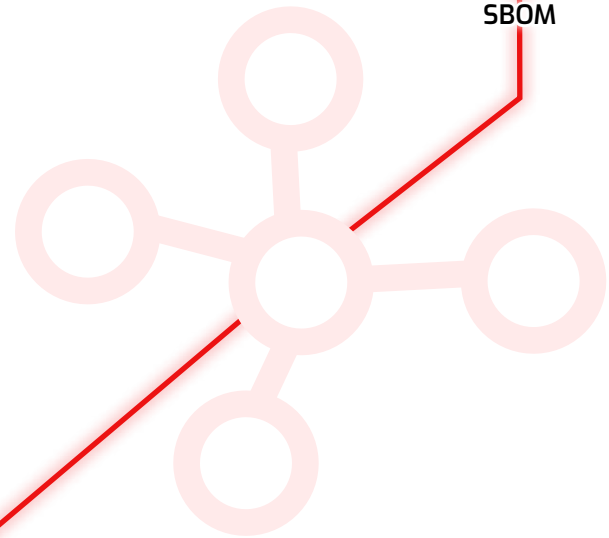
? Do I have Log4j? If so, where?

? Does any of my software have malicious contributors?

? Which devices in my network contain hard-coded or weak credentials?

SBOM

If you're not sure, you're not alone. Most financial services institutions today rely on opaque software systems that legacy application security solutions can't see.

🔧 Traditional third-party risk tools and vendor self-attestations provide limited visibility and rely on trust. They don't reveal what's actually inside the software your institution buys and operates.

Vendor-supplied SBOMs, often inaccurate due to undocumented builds and shifting dependencies, expose you to unexpected 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 financial infrastructure. Why accept it for your software?

## Where Verification Starts, and Security Follows

Financial institutions depend on a complex mix of 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 banking, insurance, and network environments.
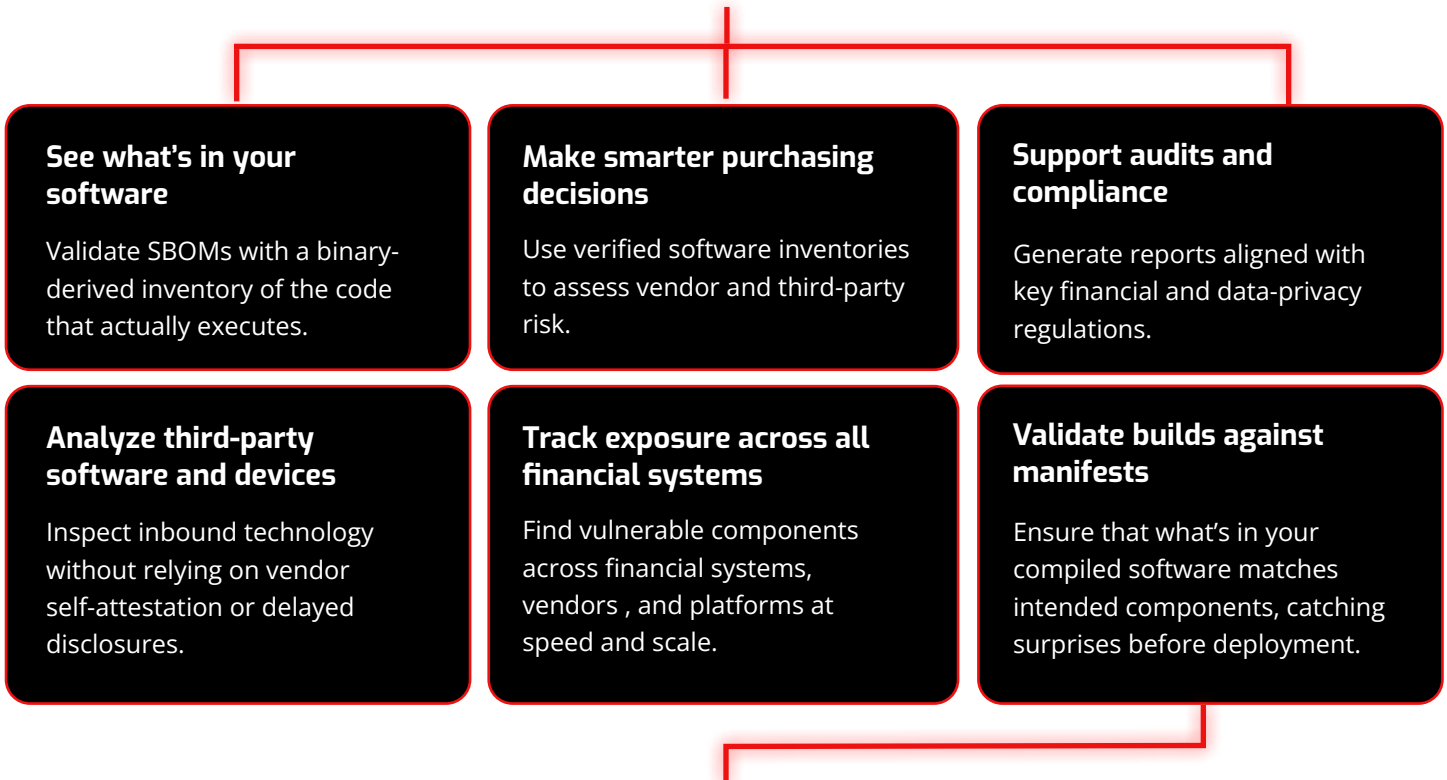
THE SOLUTION

NetRise for Those Who Buy, Use, and Maintain Software

NetRise is redefining software supply chain security for financial services institutions. By analyzing compiled code—including firmware in networking devices—NetRise creates comprehensive and accurate software inventories that expose hidden risk, improve security posture, and strengthen regulatory defensibility across core banking platforms, trading systems, ATMs, and fintech integrations.
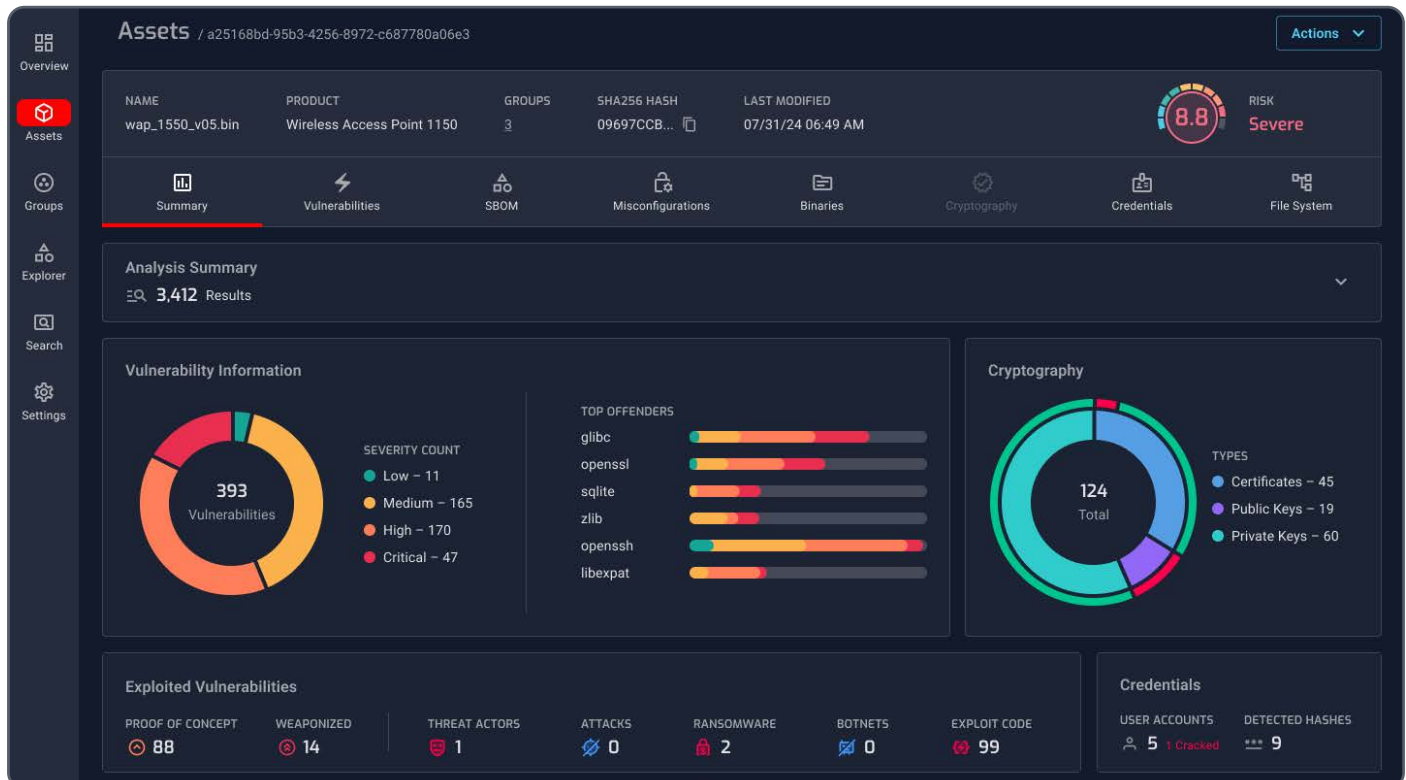
NetRise: A System of Intelligence for Finanical Software Security

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

See what's in your software

Validate SBOMs with a binary-derived inventory of the code that actually executes.

Make smarter purchasing decisions

Use verified software inventories to assess vendor and third-party risk.

Support audits and compliance

Generate reports aligned with key financial and data-privacy regulations.

Analyze third-party software and devices

Inspect inbound technology without relying on vendor self-attestation or delayed disclosures.

Track exposure across all financial systems

Find vulnerable components across financial systems, vendors , and platforms at speed and scale.

Validate builds against manifests

Ensure that what's in your compiled software matches intended components, catching surprises before deployment.

Platform Overview

Software Asset Inventory and Transparency

Build complete, accurate SBOMs that reflect what's truly in your software and devices. Capture additional artifacts such as misconfigurations, credentials, certificates, and scripts.

System of Intelligence for Software Risk

Enrich your software inventory with vulnerability context, CWEs, exploitability, reachability, and licensing indicators to prioritize and manage risk.

Binary Composition Analysis

No source required. See what actually executes in critical financial infrastructure, including networking device firmware, containers, and packaged applications.

Compliance without Bottlenecks

Deliver audit-ready evidence for key financial and cybersecurity regulations without slowing procurement, onboarding, or operations.

NetRise delivers the visibility and context financial services institutions 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 remediation.

Kernel Vulnerability Auto-Remediation
Eliminate noise with automated validation and VEX-compliant evidence, allowing teams to focus on exploitable issues and streamline audit reporting.

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

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

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.

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

Software Asset Inventory
Establish real-time, binary-derived visibility aligned with PCI DSS 4.0, SEC Cybersecurity Rules, and other financial regulatory frameworks.

Third-Party and Vendor Risk
Go beyond SBOMs to see what executes in networking devices, security appliances, ATMs, payment systems, and other third-party software—no source code required.

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

Get Started