NETRISE

What's Inside *Your* Software?

Gain visibility into the software that's running on medical devices, clinical systems, diagnostic equipment, and hospital infrastructure.

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

SBOM

THE CHALLENGE

Your SBOM Doesn't Tell the Whole Story

You rely on third-party software, medical devices, IoMT, and healthcare infrastructure across patient care areas, diagnostics, and hospital operations. How do you vet them?

Ask yourself a few basic questions:

? Do I have Log4j? If so, where?

? Am I exposed to vulnerabilities that are known to have been weaponized for ransomware attacks?

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

If you're not sure, you're not alone. Most HDOs today rely on vulnerability management and third-party risk management tools that can't answer those questions.

Vulnerability management solutions rely on publicly available databases to find risk. They don't see what's in the compiled code that executes on those devices.

Third-party risk tools and vendor self-attestations rely on trust. They don't reveal what's actually inside the software your organization buys and operates.

Critical risk lives outside the source code — in misconfigurations, credentials, and exposed keys that can become entry points for ransomware attacks.

You wouldn't tolerate that level of unknown risk in your clinical operations. Why accept it for the software that supports patient care?

SOFTWARE ASSET INVENTORY

Where Verification Starts, And Clinical Safety Follows

Your HDO depends on a complex mix of proprietary and third-party code and other artifacts in the packages that manage them.

To manage risk and satisfy regulators, you need visibility into the compiled software that actually executes in your medical devices, clinical systems, and hospital networks.

THE SOLUTION

NetRise for Those Who Buy, Use, and Maintain Software

NetRise creates comprehensive and accurate software inventories that expose hidden risk, improve security posture, and strengthen regulatory defensibility across imaging systems, patient monitors, lab equipment, and other critical clinical technologies.
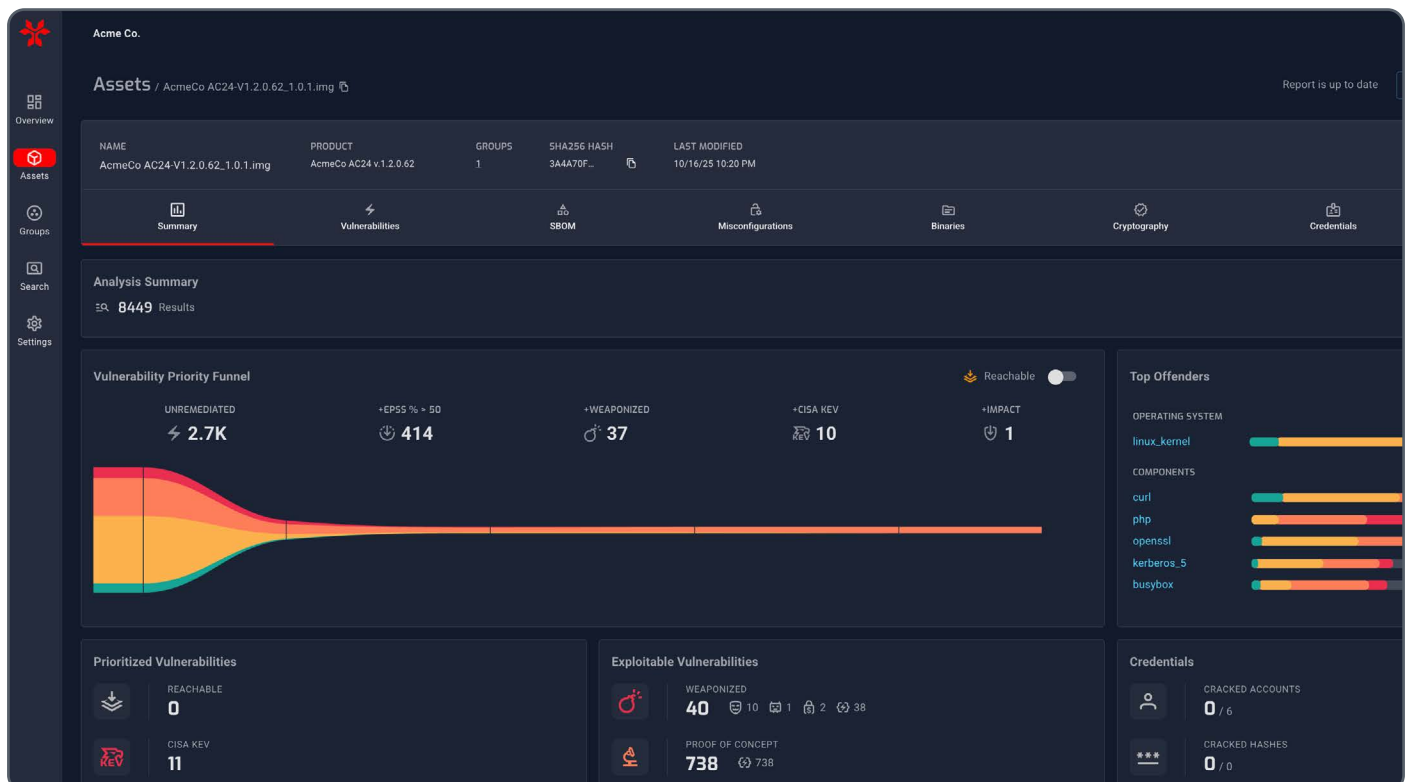
NetRise: A System of Intelligence for Enterprise Software Security

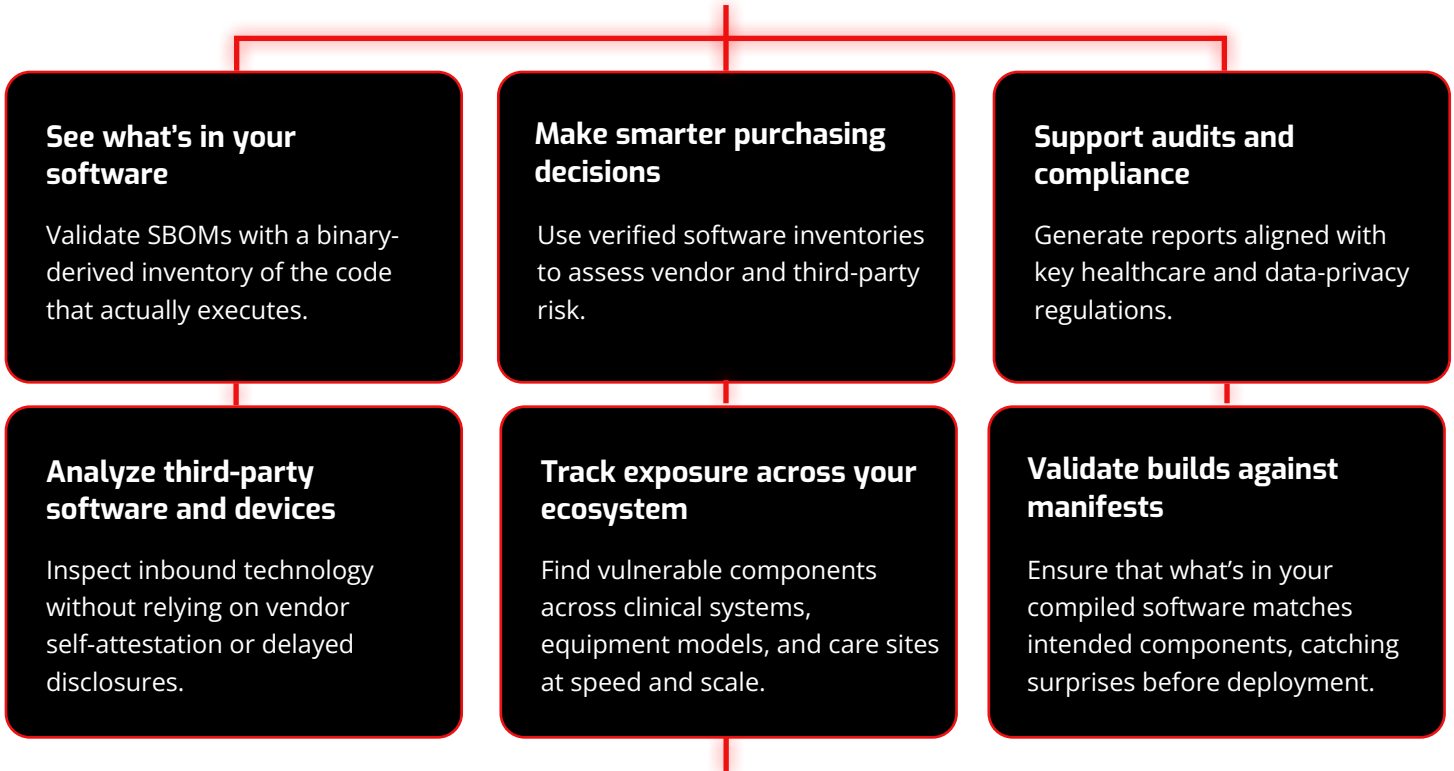Whether you manage medical devices, deploy third-party clinical systems, or oversee hospital infrastructure, NetRise helps you:

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 healthcare 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 your ecosystem

Find vulnerable components across clinical systems, equipment models, and care sites 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 Composition 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 healthcare infrastructure, including networking device firmware, containers, and packaged applications.

Compliance Without Bottlenecks

Deliver audit-ready evidence aligned to HIPAA safeguards, Joint Commission accreditation, FDA medical device cybersecurity guidance, and NIST CSF / HHS 405(d)—while also supporting PCI DSS requirements for payment systems.

NetRise delivers the visibility and context HDOs 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.

Non-CVE Risk
Surface non-vulnerability risk around misconfigurations, credentials, keys, and licenses.

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

Key Use Cases

Threat Response and Mitigation
Locate, prioritize, and remediate exposure 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 what executes in your environment. No source code required.

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

Software Asset Inventory
Establish real-time, binary-derived visibility aligned with regulatory standards.

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

Ready to see what actually executes in your environment?

Let's Find Out