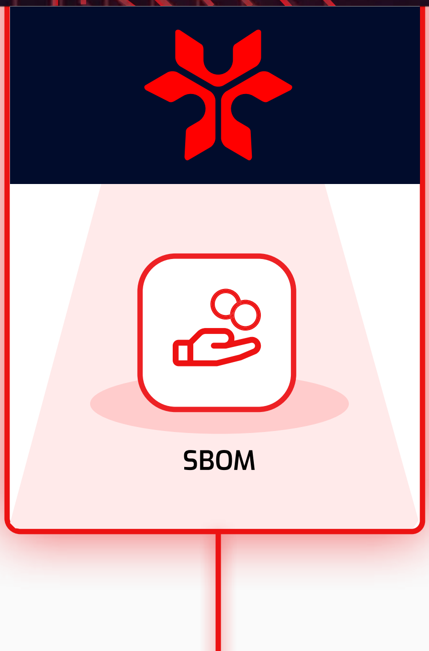
HDO OEM
Solution Brief

NETRISE

Your Executable Code Hides Risk You Can't See

Protect your organization, patient trust, and regulatory standing by verifying that the executable code in your patient facing, clinical, and operational software matches what's documented in your Software Bill of Materials (SBOM).

> Illuminate hidden risk in compiled software powering your web and mobile apps, clinical platforms, integration services, digital front door experiences, and hospital 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 vulnerabilities and components that aren't visible in SBOMs or testing tools can be included in your compiled code. Binary analysis illuminates this risk so that you can address it before you're targeted by ransomware and other high-impact attacks.

- 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 show regulators, auditors, and leadership exactly what's inside the systems you build and deploy for patient care, operations, or clinical workflows?

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 healthcare delivery organizations, these blind spots create operational risk, clinical safety concerns, regulatory exposure, and the potential for ransomware-driven service disruptions or shutdowns.

Why You Need a Comprehensive SBOM

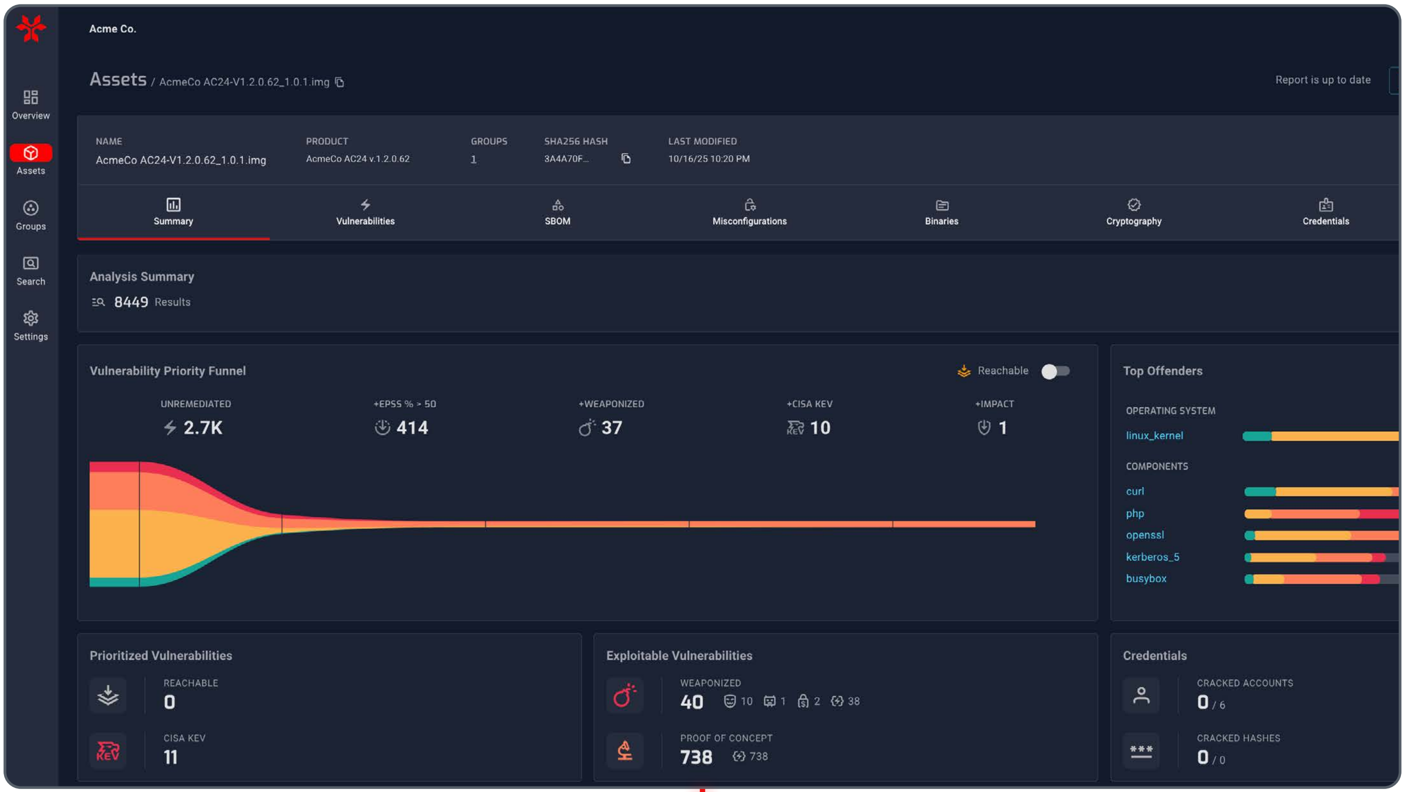
Software today is more assembled than written. Research shows that as much as 80% of today's software is derived from third-party components. A single application can include proprietary code, open-source libraries, config files, operating systems, credentials, and more.

THE SOLUTION

NetRise: Software Supply Chain Security for Healthcare Delivery Organizations

NetRise gives HDOs complete visibility into the software you build or customize internally so you can uncover hidden risk, strengthen 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.



Acme Co.

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

Report is up to date

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

Top Offenders

OPERATING SYSTEM

linux_kernel

COMPONENTS

curl

php

openssl

kerberos_5

busybox

Prioritized Vulnerabilities

REACHABLE 0

CISA KEV 11

Exploitable Vulnerabilities

WEAPONIZED 40 10 1 2 38

PROOF OF CONCEPT 738 738

Credentials

CRACKED ACCOUNTS 0 / 6

CRACKED HASHES 0 / 0

NetRise: A System of Intelligence for HDO Software Security

Whether you build clinical applications, internal operational tools, patient-facing digital experiences, middleware, or the software that powers your FHIR/HL7 integrations, as well as other software that supports clinical and business operations, 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.

Reduce exposure to real-world attacks

Correlate vulnerabilities with threat intelligence, including data on vulnerabilities exploited in ransomware campaigns, to prioritize remediation on components most likely to be targeted.

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,credentials, keys, and more.

Binary Composition Analysis

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

Software System of Intelligence

Enriched vulnerability context, including references to the CVE source, advisories, severity metrics, plus reachability, and weaponization status to prioritize risk in your environment.

Compliance Readiness

Aligned to HIPAA, Joint Commission, and FDA medical device cybersecurity guidance, and NIST CSF / HHS 405(d), and PCI DSS requirements for in-scope payment systems.

NetRise delivers the visibility and context needed to build, validate, and release secure software across your health system.

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.

Common Challenges HDO Development Teams 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.not visible through source scans.
You need audit-ready documentation.	**Provide** clear, regulator-friendly reports to support compliance with healthcare cybersecurity expectations.

What's inside *your* software?
Build trust, improve patient safety, and meet regulatory expectations with NetRise.

Let's Find Out