NETRISE

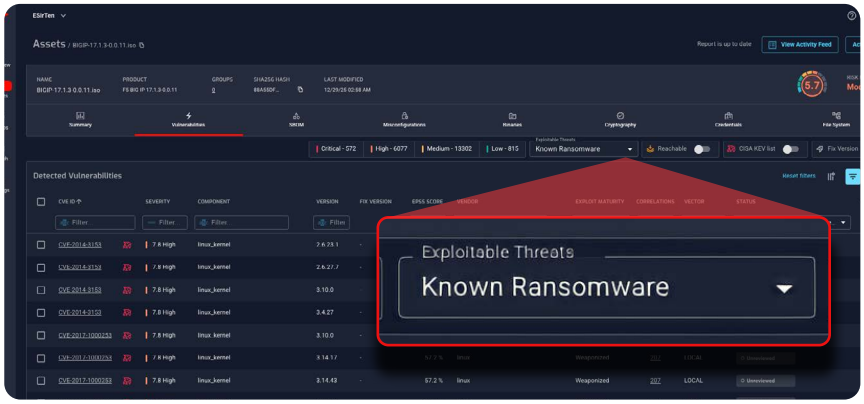
Data Sheet

What's Inside *Your* Software?

Protect patient data and clinical operations by analyzing compiled code inside medical devices, IoMT, hospital infrastructure, and patient-facing applications, without needing source code to validate what's inside.

NetRise provides deep visibility into compiled software across medical devices, IoMT, imaging and diagnostic systems, hospital network infrastructure, and web and mobile apps you use to communicate with your patients and providers—helping healthcare delivery organizations (HDOs) identify and manage software supply chain risk to ensure resilient clinical operations and regulatory compliance.

Why NetRise Is Different



Rather than relying on source-code analysis as vulnerability management tools and third-party risk programs do, NetRise analyzes compiled software running on your network, finding risk in components beyond what is found in source code analysis.

- **Non-CVE Risk:** There's more to software risk than security flaws in source code. We identify misconfigurations, hard-coded secrets, public and private key pairs, and more.
- **Comprehensive and Accurate SBOMs:** Vendor SBOMs derived from source code miss what's actually in the code that executes. NetRise finds risk in binary code, giving you an edge when negotiating with vendors.
- **Prioritize Vulnerabilities Exploitable by Attackers:** Focus on CVEs that are network accessible, in components that auto-run at startup. Quickly uncover exploits used in ransomware and other high-impact campaigns.
- **Integrations:** NetRise integrates into your workflows and into other tools used in your SOC or your Software Development Lifecycle.

Binary Composition Analysis

Uncover secrets, misconfigurations, and public and private keys from compiled software components.

SBOM Management

Generate, enrich, and validate SBOMs for full transparency across all software components.

Execution-Aware Reachability

Identify which components actually execute, under what conditions and privileges, filtering dormant vulnerabilities to focus remediation on real, exploitable attack surfaces.

Compliance & Audit Readiness

Provide evidence aligned to HIPAA technical safeguards, FDA medical device cybersecurity expectations, and NIST-based healthcare frameworks, while also supporting PCI DSS requirements for in-scope payment systems.

Vulnerability Intelligence

Gain deeper context into findings by identifying which vulnerabilities are both accessible via the network and configured to execute at startup.

Tailored Solutions for Your Role

For Internal Software Builders

(Health System Application Teams, Platform Engineering, Digital Health, Integration & Middleware Teams)

- Catch build-time deviations and unauthorized changes. The library version you think you've included may not be what was linked in your build.
- Identify and prioritize mitigation of CVEs that have been leveraged in ransomware and other high impact attacks.
- Find and prioritize vulnerabilities that are reachable via the network and autorun at startup.
- Gain visibility into legacy software components used in core platforms, where source code may be unavailable.
- Demonstrate compliance with regulatory frameworks.

For Those Who Buy, Use, and Maintain Devices

(Hospitals & Health Systems, Biomedical Engineering, Clinical Operations, Security & Compliance Teams)

- When incidents occur, confidently answer in minutes the question: Are we exposed?
- Build and maintain a comprehensive software asset inventory.
- Verify risk in vendor devices and software rather than relying on self-attestation.
- Expose hidden risk such as hard-coded secrets, misconfigurations, and public and private keys, which can provide root access across your network.
- Prioritize mitigation based on known ransomware exploits associated with operational systems.

Deploy with Ease

Start Scanning in Minutes
Get visibility into software assets almost immediately.

API-First Design
Integrate into build pipelines, CMDBs, and risk systems.

Cloud-Native
Scale easily without infrastructure overhead.

Broad OS Support
Analyze Linux, Windows, and RTOS.

Explore Platform Coverage

The NetRise Platform Coverage Sheet provides a detailed look at supported binaries, firmware formats, OS targets, and embedded components—so you know exactly what NetRise can analyze.

Who Uses NetRise?

Hospitals & Health Systems: Reduce risk in clinical devices and patient-facing web and mobile apps to avoid impact on patient care.

Biomedical Engineering Teams: Validate SBOMs and prioritize high-risk medical device vulnerabilities.

Healthcare SOCs: Triage vulnerabilities in embedded systems with exploitability context.

Regulatory Compliance: Generate audit-ready documentation for FDA, HIPAA, and Joint Commission.

Internal Development Teams: Ensure patient-facing apps ship with accurate SBOMs and no hidden supply chain risk before deployment.

What's Inside *Your* Software? Let's Find Out