Case Study

NETRISE

Gaining Device Software and Component Visibility at a Global Asset Management Firm

Background

A leading global asset management firm manages trillions of dollars across offices on multiple continents. Its network relies on thousands of third-party devices, including firewalls, virtual private network (VPN) concentrators, branch routers, security cameras, and network access control systems. Despite a mature vulnerability management program, the firm lacked automated visibility into the device software and component inventory inside these systems. Vendor documentation was incomplete, and manual audits were time-consuming and inconsistent.

Challenge

The security and risk teams needed to:

- Build a comprehensive inventory of components and libraries inside all vendor devices.
- Uncover vulnerabilities, secrets, and outdated modules hidden within device software.
- Verify vendor claims without relying on source code access or questionnaires.
- Produce evidence for compliance and audit reviews while monitoring for drift as software changed over time.

Solution

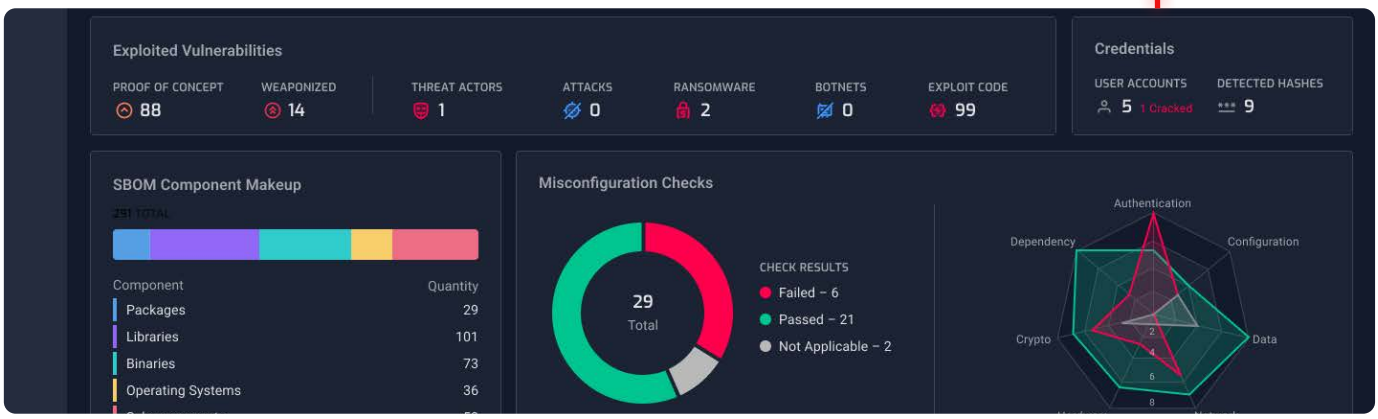
The firm deployed the NetRise Platform and uploaded firmware and device software from more than 278 assets, including critical IoT and OT appliances. NetRise extracted component inventories, identified Common Vulnerabilities and Exposures (CVE), located hard-coded keys and secrets in device software, and mapped third-party libraries. The results gave security teams objective, actionable data they could use during procurement, vendor assessments, and ongoing monitoring. The firm updated governance, risk, and compliance (GRC) workflows to require NetRise scans during onboarding and renewal.

Outcomes

Within the first 90 days, the firm identified hundreds of previously unknown vulnerabilities, including those listed in the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) catalog, as well as outdated software components across critical devices and with high EPSS Ratings. Using NetRise, the security team produced machine-generated evidence for internal audits and regulatory reviews, giving leadership clear visibility into vendor-related exposure. These findings directly informed procurement and compliance decisions, strengthening the organization's overall security posture.

Using NetRise, the security team produced machine-generated evidence for internal audits and regulatory reviews, giving leadership clear visibility into vendor-related exposure.

Why It Matters



The firm moved from relying on vendor claims to verifying device software and firmware directly. NetRise gave risk and security teams clear component visibility, measurable vulnerability data, and regulatory defensibility—without requiring source code or slowing procurement.

See how binary analysis enhances software supply chain visibility.

Learn More