

runZero for Vulnerability Management

# Protect the unseen. Secure the unscanned.

## Scan limits shouldn't define your security boundaries

Vulnerability scanners are great — for what they can reach. But what about the assets they can't? The unknown, the unmanaged, the scan-sensitive OT and IoT devices that slip through the cracks? Attackers see them, even if your tools don't.

And when scanners do find issues, they're obsessed with CVEs — overloading you with alerts while missing the bigger picture of exposures that actually matter.

Let's face it — today's threats demand more than yesterday's tools. You need vulnerability management to see everything so you miss nothing. Because if you can't see the risk, you can't stop the attack.

With runZero's Exposure Management platform, nothing is left to chance. Our agentless, authentication-free discovery covers every asset across your attack surface — IT, OT, IoT, and even the unknowns. You're taking vulnerability management where others won't, to uncover the risks they can't.

With our advanced fingerprinting, you'll go deep — mapping every attribute of every device to expose not just conventional vulnerabilities but previously hidden security issues.

And prioritization? Not a problem. Our deep, contextualized data gives you laser focus on the threats that matter, cutting the one metric that counts the most — minimizing the window of exploitability.

## Vulnerability management challenges at a glance

### Hidden targets



**60%** of assets go undetected & unmanaged — the origin of 70% of attacks.<sup>1</sup>

### Unscanned = unsecured



**42%** of devices lack agents, so they are invisible to scanners — yet they account for 64% of high-level risks.<sup>2</sup>

### Sensitive OT & IoT



**74%** of IoT & **33%** of OT devices have critical vulnerabilities but go unassessed due to their sensitivity.<sup>2</sup>

### Beyond CVEs



**15,000** exposures threaten the average organization, yet CVEs account for only 11% of critical risks.<sup>3</sup>

### Prioritization matters



**98%** of exposures, even if exploited, won't impact critical assets or key attack paths.<sup>3</sup>

1. 2022 IBM State of Attack Surface Management. 2. 2024 Order Rise of the Machine Report. 3. 2024 XM Cyber: State of Exposure Management.

The overall experience has been fantastic. It has really provided a lot of insight into our environment, insight we didn't know we needed. We thought we had great coverage and thought we knew what was on our network until we ran runZero. It helped us identify some significant gaps that we took care of.



**Chris Nadeau**

VP of Information Security,  
Granite Advance

### No Limits. No Blind Spots.

runZero goes where agents can't to find the assets they miss

- No agents or authentication needed
- Active scanning, passive discovery & API integrations
- Complete visibility into IT, OT, IoT, mobile, & cloud attack surfaces
- Identifies unmanaged & unknowns

### Every Device. Every Risk.

runZero looks beyond CVEs to reveal the risks vulnerability scanners overlook

- Advanced device fingerprinting reveals deep, hidden risks
- Covers missed security gaps
- Third-party integrations to enrich data
- Accelerates zero-day threat response, no rescans required

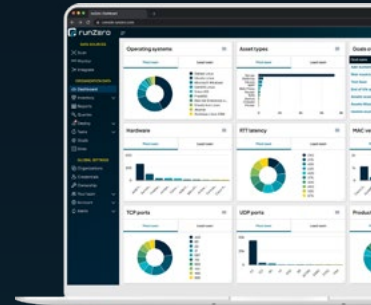
### No Noise. Just Real Threats.

runZero's meaningful data removes guesswork for focused remediation

- Contextual risk scoring by device function, location, & interconnections
- Maps exposed devices & connections
- Accelerates remediation with clear guidance & easy inquiries for quick threat resolution

## Go where others can't to secure what they miss

Other tools promise to find vulnerabilities and keep you compliant, but leave gaps — missing assets, exposures beyond CVEs, and endless management headaches. runZero uncovers risks where others can't — no agents, no credentials, no blind spots. Just complete visibility with no vulnerability left unchecked — getting you from discovery to mitigation faster.



Deployment & Management	Attack Surface Coverage	Exposure Detection	Actionable Insights	Compliance
<b>runZero</b>				
Bypasses agents and authentication limits, freeing resources & effortlessly revealing hidden network risks.	Discovers all network assets — internal, external, IT, OT, & IoT — including unmanaged & unknown devices.	Exposes all attacker targets beyond CVEs — misconfigurations, segmentation gaps, missing security controls, & OT/IoT weaknesses.	Prioritizes risks using precise data on asset attributes, interconnections, & business context, for faster mitigation.	Meets regulatory demands while ensuring full visibility and vulnerability coverage for assessments and planning.
<b>Other Solutions</b>				
Burdens you with agents & authentication hurdles, wasting time & limiting vulnerability management.	Limits visibility to a fraction of attack surfaces, missing unknown devices & leaving exploitable blind spots.	Fixates on CVEs, creating a false sense of security while attacker opportunities are overlooked.	Relies on theoretical scoring, ignoring asset context & prioritizing low-impact risks over real threats.	Misses exposures, only partially meeting regular requirements — risking fines or extra tool investments.



runZero delivers the most complete security visibility possible, providing organizations the ultimate foundation for successfully managing exposures and compliance. With a world-class NPS score of 82, runZero has been trusted by more than 30,000 users to improve security visibility since the company was founded by industry veteran HD Moore. Learn more on our [website](#).

Test drive the runZero Platform for 21 days, with an option to convert to our free Community Edition at the end of your trial.

[Try runZero for Free](#)