runZero for Cyber Readiness Assessments

runZero helps organizations pass cyber readiness assessments without surprises, using defensible evidence of what's actually on their network.

Assessment reality: unknown assets undermine readiness

Unknown and unmanaged devices undermine cyber readiness long before an assessment begins. In modern environments spanning IT, OT, and IoT systems — including segmented and air-gapped networks — maintaining an accurate inventory of network-connected assets is increasingly difficult. Agent-based and credential-dependent tools leave gaps, while aggregated data from disparate security platforms often produces an incomplete or inconsistent picture.

Cyber Operational Readiness Assessments such as CORA, JCIP, and CCRI are designed to surface those gaps. Assets that fall outside endpoint protection, vulnerability scanning, directory services, or boundary controls indicate a loss of visibility and control. When organizations cannot confidently account for what is connected to their network, assessments expose unmanaged risk rather than confirm readiness.

runZero for assessment-grade visibility

You can't secure what you can't account for.
Assessment readiness depends on visibility that does not rely on assumptions, credentials, or pre-existing tooling. runZero discovers and fingerprints network-connected assets using native, unauthenticated methods, providing a defensible view of known, unknown, and unmanaged assets across internal and external environments. By combining proprietary active scanning with passive network traffic sampling, runZero is the only tool that identifies assets without depending on agents, APIs, or external data sources.

This approach enables fast, accurate discovery across IT, OT, and IoT systems, including environments that are segmented, restricted, or air-gapped. Safe to use even with fragile OT systems, runZero delivers high-fidelity asset fingerprinting using almost 1,000 attributes, allowing organizations to validate inventories and reconcile discrepancies before they are challenged during an assessment. The result is a clear, evidence-based understanding of the attack surface that assessments require to confirm cyber readiness.

Get prepared. Reduce risk. Avoid surprises.

- Cyber Operational Readiness Assessment (CORA)
- JWICS Cyber Inspection Program (JCIP)
- Command Cyber Readiness Inspection (CCRI)

How runZero supports assessment preparation

Establish a defensible asset inventory

runZero enables organizations to demonstrate an accurate, evidence-based view of what is connected to their network by:

- Discovering unknown and rogue assets through native, unauthenticated scanning.
- Identifying internal, boundary, and externally facing systems.
- Revealing assets missing endpoint protection, vulnerability scanning, or directory management, highlighting control coverage gaps.
- Identifying end-of-life systems, where unsupported software introduces unmanaged risk.
- Identifying high-risk assets to support effective prioritization of remediation efforts.
- Rapidly querying exposure to newly disclosed and zero-day vulnerabilities without rescanning, using runZero Rapid Response queries.

Validate network segmentation

runZero enables organizations to validate segmentation in practice by:

- Providing full RFC 1918 network coverage.
- Tracing route paths between subnets, exposing actual connectivity rather than assumed design.
- Identifying unintended connections and network bridges, where segmentation controls may be bypassed.
- Detecting segmentation decay across complex environments, as networks evolve over time.

Verify externally facing assets

runZero supports external attack surface accountability by:

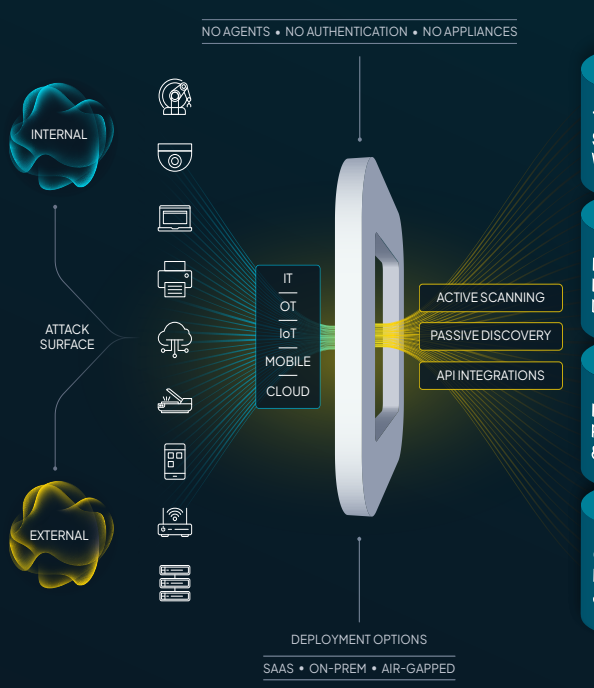
- Scanning public IP ranges, domains, and ASNs to enumerate externally reachable assets.
- Identifying exposed services and misconfigurations that increase external risk.
- Correlating external findings with internal asset inventories to provide a unified view of the entire attack surface.
- Supporting reconnaissance and validation for offensive and red-team activities, using the same high-fidelity fingerprinting applied during assessment preparation.

Extend assessments into continuous readiness

runZero enables assessment findings to persist beyond inspection windows by:

- Continuously identifying newly introduced assets to prevent new blind spots emerging
- Reducing time to detection for CVEs and zero-day exposures, shortening the incident response lifecycle
- Sharing authoritative asset data with SIEM, CMDB, and other security and IT tools

See & Secure Total Attack Surface



TOTAL ATTACK SURFACE VISIBILITY

- → Discover every IT, OT, & IoT asset, including unknowns
- → Unify visibility across internal & external attack surfaces
- → Fingerprint every asset with unmatched depth & accuracy

FULL-SPECTRUM EXPOSURE DETECTION

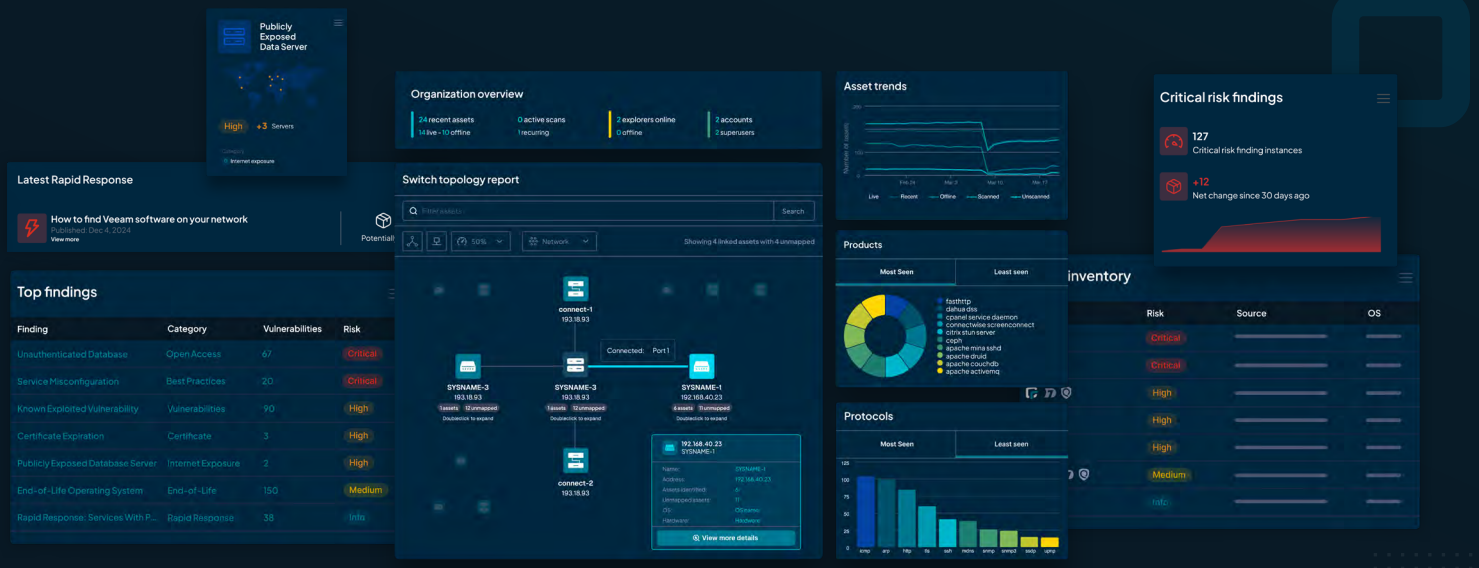
- → Detect broad classes of exposures missed by other tools
- → Respond to 0-days instantly without rescanning
- → Detect true risks with unauthenticated vuln scanning

RISK PRIORITIZATION & INSIGHTS

- → Prioritize critical exposures with data-driven risk findings
- → Accelerate remediation with AI-augmented guidance
- → Gauge impact with asset context & detailed attributes

COMPLIANCE, REPORTING, & KPIs

- → Comply with requirements for discovery & monitoring
- → Accelerate & streamline compliance reporting
- → Track security posture with goals & improvement metrics



runZero provides a single source of truth for exposure management across your total attack surface: internal, external, IT, OT, IoT, mobile, and cloud. Providing the most complete and accurate visibility into every asset and exposure, runZero helps you mitigate risks faster, meet compliance requirements, and ensure you continuously discover the assets and exposures that others miss. 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