runZero

EXPOSURE MANAGEMENT

runZero for NIS2 Compliance

Know your attack surface. Prove your compliance.

You can't secure — or prove — what you can't see

Only 16% of organizations subject to NIS2 are confident they fully comply — despite enforcement already being active across 18 sectors. Yet non-compliance risks fines of up to €10 million or 2% of global annual turnover. And for the first time, management bodies face personal liability for failures, not just their organizations.

Every NIS2 minimum security measure starts with the same foundation: complete visibility across your attack surface — every asset, every exposure, every risk. Without it, you cannot demonstrate the risk management, incident preparedness, or supply chain controls NIS2 requires.

Legacy tools can't deliver that visibility. They miss unknown and unmanaged devices (the starting point for 74% of cyber attacks), aren't suitable for fragile OT environments, and stop at the protocol gateway — leaving the PLCs and field devices behind it invisible to defenders and potentially exposed to attackers. In a sample set of manufacturing environments, runZero found that 30% of OT assets sit one hop from an internet-exposed device. 90% are within two hops.

runZero finds every asset and exposure across IT, OT, IoT, cloud, and mobile — even in air-gapped environments. No agents. No credentials. No disruption. One continuously refreshed source of truth, with the data and reporting to prove NIS2 compliance.

NIS2 compliance risks at a glance

Compliance gap

Only 16% of in-scope organizations are confident they are fully compliant. [1]

Financial penalties

€10 million or 2% of global turnover in maximum fines. [2]

Personal stakes

Management bodies held personally liable for cybersecurity failures under NIS2, not just organizational fines. [3]

Blind spots exploited

74% of successful cyber attacks stem from hidden or unmanaged assets. [4]

Hidden OT exposures

30% of OT assets are only one hop away from an internet-exposed device, and 90% are within two hops. [5]

1. CyberSmart 2. NIS2 directive 3. NIS2 directive 4. TrendMicro 5. runZero

> 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

See Everything, Miss Nothing

runZero finds what other tools can't, including the assets you don't even know to look for.

- Agentless active scanning, passive discovery, and API integrations
- Sub-asset discovery behind Modbus, BACnet, EtherNet/IP, and KNXnet gateways
- Full internal and external attack surface coverage — IT, OT, IoT, mobile, cloud, and air-gapped
- Unknown and unmanaged device discovery
- Deep device fingerprinting across 220+ protocols, providing rich, contextualized asset data

Uncover Critical Risks, Prioritize What Matters

runZero surfaces the exposures and segmentation gaps NIS2 requires you to find — and fix.

- Attack path mapping from initial compromise to operational impact
- Multi-homed device and segmentation bypass detection
- Exposure detection beyond CVEs — misconfigurations, weak protocols, expired certificates, and more
- Third-party and vendor-managed asset visibility for supply chain compliance
- Business-context risk prioritization
- Zero-day threat response without rescans

Meet Core Requirements, Prove Your Controls

runZero gives you what NIS2 demands — continuous, verifiable proof for regulators, auditors, and your board.

- Continuously refreshed asset inventory for audit-ready evidence
- Asset and exposure data to scope and report incidents within NIS2 24/72-hour windows
- Compliance reporting which can be mapped to NIS2 Article 21 minimum measures
- Change tracking and drift detection
- Continuous monitoring evidence for management body accountability

U.S. government confirms:
runZero is safe and effective in OT environments

The U.S. Department of Energy's National Renewable Energy Laboratory (NREL) found runZero detected all IP-addressable OT assets — including devices communicating over Modbus — with no measurable impact on ICS performance and no interference with SCADA processes. NREL noted this directly challenges the assumption that active scanning disrupts OT operations.

	Deployment & Time to Discovery	Attack Surface Coverage	Exposure Management	Actionable Insights	Compliance
runZero	Deploys rapidly with no agents, authentication, or appliances, giving you full asset & exposure visibility in hours.	Finds every asset for unified visibility across your total attack surface — eliminating blind spots that increase compliance risks.	Goes beyond CVEs to surface elusive exposures such as misconfigurations, segmentation failures, weak protocols, & expired certificates.	Prioritizes risk by business impact, & quickly maps attack paths & blast radius for NIS2 24/72-hour disclosure obligations.	Provides continuously updated asset & exposure data to support NIS2 Article 21 compliance & board oversight.
Other Solutions	Consume time & resources with complex rollouts that rely on agents, appliances, & authentication.	Cover only known, addressable assets — IT or OT, rarely both — leaving critical unknowns exposed to exploitation & compliance penalties.	Fixate on CVEs, missing the broader exposure classes NIS2 requires organizations to find.	Provide fragmented data that delays scope assessment, increasing the risk of missing mandatory reporting deadlines.	Deliver partial coverage & static reports that fail NIS2's continuous monitoring requirements & won't satisfy auditors.

runZero

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 asset and exposure intelligence, 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