ZERO. Networks

How Zero Networks Helps with NIS2 Regulation Requirements

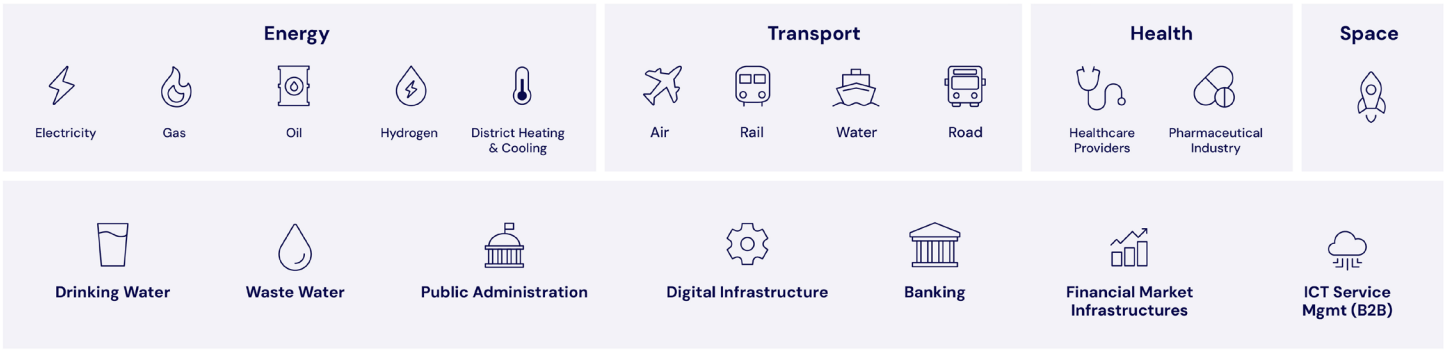
Network and Information Systems (NIS) Directive 2022/2555, otherwise known as NIS2, recently replaced its predecessor, Directive 2016/1148 or NIS1, in order to expand the original NIS directive. Though the first directive was successful as a catalyst for institutional and regulatory cybersecurity change, it came short in addressing current and emerging cybersecurity challenges.

The goal of NIS2? Protect critical infrastructure and essential services in order to keep the economy – and society – humming along without detrimental disruptions. The NIS2 directive sets a more ambitious baseline for cybersecurity risk management across a much wider scope with stronger supervision.

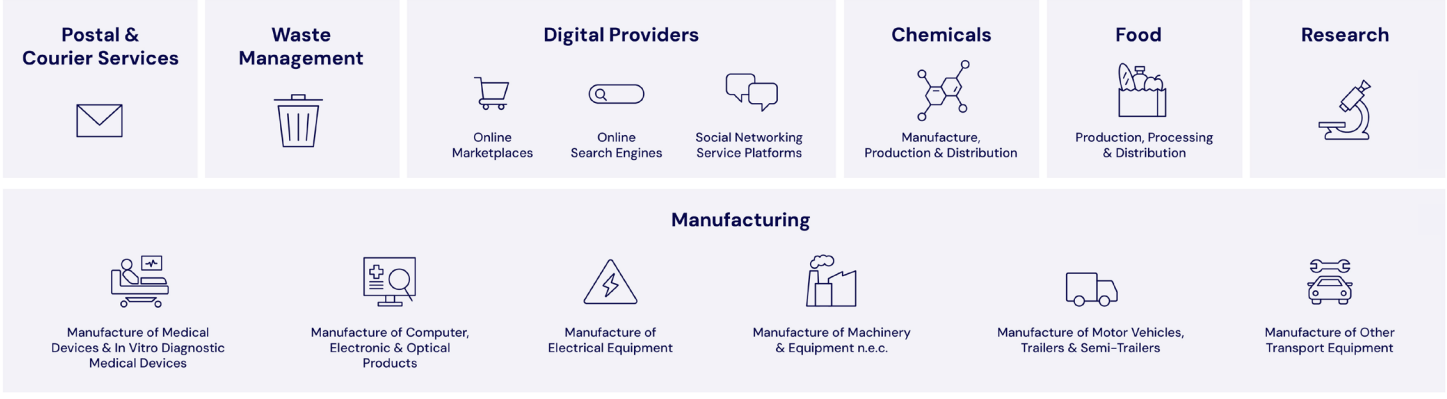
The new directive identifies more sectors as critical or "Essential"; while NIS1 enveloped about 8 sectors, NIS2 covers 18 sectors. This broadened scope pulls more medium- and large-sized organizations across the EU under NIS2 regulation for the first time. The directive also identifies a second tier of sectors as "Important" entities, which are now being held to cybersecurity standards as well – though these are slightly less stringent than those of their Essential peers.

Aside from a broadened scope, organizations must implement documented, risk-based security controls covering access control, supply-chain security, vulnerability management, governance, and incident response. They are also legally required to report significant cyber incidents within strict deadlines. Failure to comply will result in sizeable fines and non-monetary enforcement measures.

Essential Business Sectors



Important Business Sectors



Who Must Comply

Organizations must comply with NIS2 if it operates in the EU (or provides services into it), falls within a covered sector, and either meets the size thresholds or is deemed critical regardless of size.

Under NIS2, most organizations are in scope if they have 50+ employees or €10m+ turnover/assets, whether classified as essential or important. Certain critical service providers are included regardless of size, and smaller entities may still be designated in scope by national authorities if they are essential to societal or economic stability.

Specific requirements where Zero Networks can help you achieve NIS2 compliance:

Requirement	Description	How Zero Helps	Impact
Governance & Management Responsibility *Relevant Article: Article 20*	Leadership must ensure the approval, oversight, and implementation of cybersecurity controls, and demonstrate measurable risk reduction and governance effectiveness.	Zero provides automated and enforceable controls that reduce lateral-movement exposure, restrict internal pathways, and generate audit-ready evidence showing that approved controls are active and effective.	Strengthens executive accountability by providing measurable security outcomes, documented enforcement, and defensible proof of operational control effectiveness.
Cybersecurity Risk Management Measures *Relevant Article: Article 21(1) and Article 21(2)*	Organizations must implement proportionate technical and organizational security measures that protect systems throughout the full lifecycle—prevention, detection, response, and recovery.	Zero enforces identity-based microsegmentation and deterministic isolation across all assets, preventing unauthorized internal communication and limiting incident propagation.	Directly reduces cyber risk by minimizing attack surfaces and containing compromise events, supporting full-spectrum risk-management objectives.
Access Control & Identity Protection *Relevant Articles: Article 21(2)(g) and Article 21(2)(i)*	Access to systems must be restricted to authorized users, devices, and services. Privileged access requires strict control and protection from credential theft or misuse.	Zero enforces identity-based access policies across all human and machine identities, applies MFA at the network layer, and ensures least-privilege access for privileged accounts and service accounts.	Reduces credential-based compromise, privilege escalation, and unauthorized access pathways across the environment.
Network & Information System Security *Relevant Article: Article 21(2)(f)*	Organizations must secure internal network communications and prevent lateral movement, ensuring the integrity, confidentiality, and resilience of internal systems.	Zero blocks unauthorized east-west traffic, isolates critical systems, eliminates unnecessary exposure, and prevents lateral movement—even if an attacker compromises an endpoint.	Increases internal network resilience, prevents threat propagation, and ensures critical systems remain protected even during active incidents.
Supply Chain & Third-Party Security *Relevant Article: Article 21(2)(e)*	Cybersecurity risks arising from service providers, vendors, and external partners must be identified, monitored, and minimized.	Zero restricts third-party access to only required assets and ports, applies identity-based controls, and prevents vendors from moving laterally through internal systems.	Reduces supply-chain blast radius, prevents unauthorized access through vendor accounts, and ensures traceable, least-privilege external connectivity.

Incident Handling & Containment *Relevant Articles: Article 21(2)(b) & Article 21(2)(c)*	Organizations must maintain capabilities for detecting, managing, and containing cybersecurity incidents while supporting business continuity.	Zero enables real-time isolation of compromised systems and enforces segmentation that keeps unaffected systems operational during an active attack.	Shortens incident duration, prevents escalation, and protects operational continuity during security events.
Vulnerability Handling & Exposure Reduction *Relevant Article: Article 21(2)(d)*	Organizations must reduce exposure to known vulnerabilities, especially when patching or remediation cannot be performed immediately.	Zero isolates vulnerable or legacy systems, restricts communication pathways, and prevents unpatched systems from being used as pivot points.	Minimizes exploitation risk, provides compensating controls for unpatchable assets, and prevents vulnerable systems from escalating compromises.
Business Continuity & Operational Resilience *Relevant Article: Article 21(2)(c)*	During cyber incidents, organizations must ensure the availability and continuity of essential services.	Zero's segmentation architecture prevents threat spread and isolates compromised assets without shutting down the environment.	Ensures critical services remain online and operational even when parts of the environment are under attack.
Incident Reporting Obligations *Relevant Article: Article 23*	Significant incidents must be reported within strict timelines (24h early warning, 72h notification, final report in 1 month). Accurate scoping and impact analysis are required.	While Zero does not perform regulatory reporting, it provides deeper, documented visibility of every asset and identity on a network and all traffic. This can provide security teams with detailed attack paths and containment visibility. This can support accurate incident scoping, faster impact assessment, and stronger forensic evidence for NIS2 reporting obligations.	Improves accuracy and completeness of incident notifications, supports forensic investigations, and documents containment boundaries for compliance.

Connect with the Zero team to discover how you can streamline your NIS2 compliance with automated, identity-based microsegmentation that deploys in just 30 days.

Request a demo

ZERO. Networks