NIS2 Compliance: Close the endpoint security gap and achieve operational resilience.

What is the NIS2 Directive?

The NIS2 Directive[1] is the European Union's cybersecurity law for organizations both public and private, with reporting in effect from January 2025, requiring proactive cyber risk management and operational resilience. Executive accountability and rapid incident reporting are mandatory. Penalties reach €10 million or 2% of global turnover, with possible personal liability for executives. Non-compliance can also lead to audits, public disclosure, or even suspension from the EU market.

Who does NIS2 apply to?

NIS2's scope is broad and applies to any organization (public or private) delivering "essential" or "important" services in the EU. Sectors include energy, water, transport, healthcare, digital infrastructure, finance, manufacturing, public administration, online platforms, and more. Non-EU companies serving EU customers must appoint an EU representative.

What are the NIS2 cybersecurity requirements?

- Continuous risk analysis and management.
- Rapid incident handling and reporting (24-hour notification, 72-hour follow-up).
- Business continuity and disaster recovery plans.
- Supply chain risk management.
- Strict access control, identity management, and multi-factor authentication.
- Patch management, encryption, data protection, and regular cyber hygiene training.
- Continuous review and improvement of security controls.

Traditional Windows/Mac endpoints require 7+ separate tools (EDR, NGAV, DLP, etc.) to tick these boxes, leading to cost, complexity, and compliance gaps. IGEL flips this with a single, secure, immutable endpoint OS.

What are the requirements for the endpoint?

Endpoints are a primary risk surface—NIS2 expects you to:

- Ensure devices are protected from malware, ransomware, and insider threats.
- Prevent local data loss or exfiltration.
- Control application execution and enforce strong authentication.
- Centralize configuration, patching, and auditing.
- Integrate with SIEM/SOC for real-time event visibility.

[1] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

How should companies start preparing?

- Assess if NIS2 applies to your organization and evaluate current cybersecurity posture vs. NIS2 requirements.
- Set up a cross-functional NIS2 group including senior stakeholders to determine strategic direction.
- Engage Leadership and make cybersecurity a board-level issue.
- Deploy Preventative Security: Move away from reactive, patch-based models.
- Centralize control of dispersed endpoints with unified management, monitoring, and recovery.
- Update policies, controls, and endpoint strategies.

How IGEL can help your business

IGEL supports NIS2 compliance without complexity or compromise on the endpoint. Simplify compliance with Article 21 mandates for technical, operational, and organizational cybersecurity risk management measures, and Article 23 to report significant cybersecurity incidents rapidly and accurately.

Preventative Security Architecture™: IGEL's immutable, read-only OS eliminates several endpoint threats (malware, ransomware, insider risk, local data loss).

No Local Data: No sensitive data stored on the endpoint means lost or stolen devices do not cause breaches.

Trusted Application Platform: Every device boots from a verified, tamper-resistant state—no unauthorized code runs.

Built-in Business Continuity: Instant failsafe options to recover endpoints and connect to critical services in minutes with IGEL Dual Boot, IGEL USB Boot, and IGEL Managed Hypervisor. Reduce downtime, no hardware replacement or reimaging required.

Universal Management Suite: Centralizes policy, updates, patching, access controls, and SIEM integration for fast audit response and real-time visibility.

Preventative Security Model™: IGEL's unifying framework and orchestration methodology. Native integration with leading IAM, SSO, and SASE partners. MFA and strong policy enforcement—all from one platform.

IGEL's modern approach to endpoint security reduces the attack surface and neutralizes entire threat categories including ransomware, insider exfiltration, and malware persistence.

IGEL's Preventative Security Model™ and Zero Trust enforcement at the endpoint increase the overall cyber security posture, significantly simplify compliance with the NIS2 Directive—while reducing audit overhead, operational costs, and user experience.

Discover how IGEL can streamline your NIS2 compliance.

Learn more about the Preventative Security Model