illumio

SOLUTION BRIEF

Achieve NIS2 Compliance With Illumio

Adopt a Zero Trust strategy to meet the requirements of NIS2

What is new in NIS2?

The purpose of cybersecurity is to build a more resilient environment in the face of inevitable breaches. This means that an organisation should be able to continue operations even while under attack — something that's especially important for essential services.

The new NIS2 directive better reflects the current cybersecurity landscape by:

- Including additional industries considered essential
- Increasing the level of cyber resilience
- Reducing resilience inconsistencies in sectors already covered by the NIS1 directive
- Improving the level of joint situational awareness and collective capability to prepare and respond.

NIS2 implementation changes

Updates to the classification of organisations. Entities that are required to comply with NIS2 are now classified as either Operators of Essential Services (OES) or Important Entities (IE). OES includes healthcare, energy, and transport; IEs include digital providers and postal and courier services.

Increases in the scale of entities that need to comply. Organisations with more than 250 employees and an annual turnover exceeding €50 million are now in scope. In particularly high-risk sectors, organisations must comply regardless of size.

Clarifying the reporting process for incidents. An incident must be reported to the local Cybersecurity Incident Response Team (CSIRT) within 24 hours.

Use Zero Trust principles for NIS2 compliance

Step 1: Identify risk

Determine each resource's level of risk to guide deployment priorities. This process includes listing all resources, mapping interdependencies, and identifying vulnerabilities.

Step 2: Protect assets based on risk

Secure resources based on risk level. This includes closing open, unused, and high-risk ports, only allowing verified communications, and limiting reach of protocols used by ransomware.

Step 3: Respond quickly

Upon breach, restrict or temporarily suspend communications to high-risk resources. Segment infected systems into a quarantined group until they can be cleaned and restored. The rest of the systems can safely operate to maintain services.

How Illumio aligns with NIS2

NIS2 focuses on standardising key cybersecurity measures, and Illumio Zero Trust Segmentation (ZTS) helps you meet the following.

Policies on risk analysis and information security

Application dependency mapping provides complete visibility into traffic across all workloads, including containers, IoT, and virtual machines, in a single console. This allows security teams to pinpoint network risks and create security policies that block unnecessary connections between ports.

Incident handling

During an active breach, Illumio can respond quickly to restrict access to critical resources, stopping the spread of an attack and fully isolating compromised systems. Post-breach, ZTS intelligently separates the infected system in real-time to allow safe restoration of data.

Business continuity and crisis management

Security and IT teams can use Illumio to set up protection around individual departments and systems so they can resume operations while shielded from the attack. Any attempts to reinfect can be prevented by only allowing connection with an immutable data source during breach recovery.

Supply chain security

Illumio allows only known and verified communication between environments. This ensures that when there's a breach in the supply chain, ZTS will stop the breach from entering and spreading into the organisation's systems.

Security in network and information systems

Illumio extends consistent microsegmentation across all environments, from on-premises data centers to hybrid and multi-cloud environments. This ensures a breach gets stopped and contained immediately so attackers cannot move to other parts of the network.

Policies and procedures to assess effectiveness of measures

The Illumio Ransomware Protection Dashboard helps better prepare and protect against the threat of attack by providing insights into workload risk exposure, visibility of protected versus unprotected workloads, and a protection coverage score.

Basic computer hygiene practices and cybersecurity training

Illumio's end-to-end visibility of the entire attack surface provides insight into security gaps that help inform cyber hygiene and training needs. ZTS also ensures that inevitable human errors don't leave vulnerabilities for attackers to exploit.

Human resources security, access controls, and asset management measures

With Illumio, security teams can implement granular segmentation policies to limit access to systems, including HR resources. This means that if one part of the network gets breached, attackers can't spread to critical resources.

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.