DEVICE-LEVEL, ZERO-TRUST
OT CYBERSECURITY

White Paper Series

The European Network and Information Security (NIS2) Directive

Industrial Operations & Critical Infrastructure Cybersecurity Regulatory Frameworks

What the latest regulations demand of European organizations in the new era of cyber risk and how the NanoLock OT Defender solution helps comply with this new legislation

INTRODUCTION

Today's manufacturing, industrial and critical infrastructure organizations enjoy unprecedented performance, agility, and efficiency. Like everything else in business, this comes at a price. As recent cyber-attacks have demonstrated, the rise of Industry 4.0 innovations and IT/OT convergence can translate to new vulnerabilities, which can lead to significant operational disruptions, safety issues, and reputational damage.

To maintain security, stability, and prosperity, regulators around the world are developing rigorous compliance frameworks that seek to minimize cyber risks while maintaining the benefits of technological advances. The European Union's NIS2 Directive is one such regulation that outlines the requirements for protecting IT and OT systems and devices, with which businesses and relevant public organizations must comply.

In this White Paper, we discuss the NIS2 directive, present the key cyber requirements, and share how a device-level, zero-trust OT cybersecurity approach can achieve operational and device security while also helping to ensure compliance.

What is the European Union NIS2 Directive?

Enacted in December 2022 and in force since January 2023, the European Union-wide NIS2 Directive is designed to improve the way the European Union Member States prevent, handle and respond to cybersecurity attacks and crises. It stipulates the implementation of up-to-date cybersecurity measures to protect IT and OT systems by all public and private entities that fulfill key functions for the economy and society across the internal market.

By October 17, 2024, all Member States must incorporate NIS2 into their national law and publish the measures necessary for compliance.

Objectives

NIS2 establishes clear responsibilities, increased cooperation, and better future planning. Its objective is to reduce inconsistencies in cyber resilience across Member States and increase the overall resilience of the continent. It delineates proactive protection and post-incident reporting requirements, sets the provisions governing member states' supervision and enforcement, and defines the capabilities of the relevant competent authorities.

The NIS2 Directive moves the Union away from a reactive cybersecurity posture to that of active protection and prevention.

Stipulations and Fines

NIS2 lists seven key elements that all relevant organizations must address and implement, including incident response, two-stage incident reporting, third party and supply chain security, and encryption and vulnerability disclosure. It also comes with a minimum list of administrative sanctions whenever organizations break the rules regarding cybersecurity risk management or their reporting obligations. The sanctions include binding instructions, the implementation of the recommendations of a security audit, bringing security measures in line with NIS2 requirements, as well as **administrative fines – up to €10 million or 2% of the entities' total turnover worldwide, whichever is higher.**

Sectors Included in NIS2 Jurisdiction

Energy, transport, banking, financial market infrastructure, health, drinking water, digital services providers, food, manufacturing, postal and courier, providers of public electronic communications network or services, ICT service management, waste water, waste management, public administrators, space, research and chemicals, among others.

Important Clauses at a Glance

- Clauses 9, 51, 57 call to adopt **active cyber protection and prevention,** rather than responding reactively, combined with the use of capabilities deployed within and outside the victim network.
- Clause 89 discusses **cyber hygiene practices such as zero-trust principles, device configuration, identity and access management.**

How a device-level, zero-trust solution can help ensure compliance

Many businesses and public entities deploy Industrial Control Systems (ICS), which include machines and devices such as Programmable Logic Controllers (PLCs) from different vendors and distributors. To achieve their production objectives, these organizations combine legacy and new equipment. They work with a significant number of third-party suppliers and outsourced contractors across different plants and countries. All this expands value while also expanding the vulnerabilities.

As cyber-attackers target organizations in a myriad different ways, existing cybersecurity approaches such as network monitoring are no longer enough to protect sophisticated heterogeneous OT environments. As the NIS2 Directive requires, protection must be prevention-based and incorporate zero trust.

NanoLock Security is shifting the paradigm from post-incident detection to proactive device-level, zero-trust prevention. It is designed to protect against outsider, insider, and third-party threats, plus human errors. It secures the integrity of OT assets regardless of vendor, whether they are legacy or new, or connected to a network, offline or air-gapped.

REGULATORY REQUIREMENTS AND THE NANOLOCK OT DEFENDER SOLUTION

Requirements	The Nanolock OT Defender Solution
Clause 32 With ICT risk becoming more and more complex and sophisticated, good measures for the detection and prevention of ICT risk depend to a great extent on the regular sharing between financial entities of threat and vulnerability intelligence. Information sharing contributes to creating increased awareness of cyber threats. In turn, this enhances the capacity of financial entities to prevent cyber threats from becoming real ICT-related incidents and enables financial entities to more effectively contain the impact of ICT-related incidents and to recover faster. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, in particular uncertainty about its compatibility with data protection, anti-trust and liability rules.	NanoLock OT Defender delivers a prevention-based solution. It prevents unauthorized users from making changes to Programmable Logic Controllers (PLC). Only authorized users created and managed by the Nanolock MoT server can change the PLC configuration based on permissions, multi-factor authentication, and predefined policies.
Clause 47 Inspired by relevant international, national and industry best practices, guidelines, recommendations and approaches to the management of cyber risk, this Regulation promotes a set of principles that facilitate the overall structure of ICT risk management. Consequently, as long as the main capabilities which financial entities put in place address the various functions in the ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving and communication) set out in this Regulation, financial entities should remain free to use ICT risk management models that are differently framed or categorized.	NanoLock OT Defender offers proactive protection and prevention by using a device-level, zero-trust architecture.
Clause 57 As part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy. Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network. This could include Member States offering free services or tools to certain entities, including self-service checks, detection tools and takedown services. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully preventing, detecting, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures.	As an addition to network-based solutions, NanoLock provides device-level protection to achieve active prevention, as opposed to post-incident detection.

Requirements	OT Defender Solution
Clause 45 Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organize training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.	NanoLock OT Defender deploys zero trust to achieve device security, whether the device is legacy or new, and whether it's online, offline, or air gapped. It offers identity and access management features to prevent credential misuse.
Clause 119 With cyber threats becoming more complex and sophisticated, good detection of such threats and their prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to an increased awareness of cyber threats, which, in turn, enhances entities' capacity to prevent such threats from materializing into incidents and enables entities to better contain the effects of incidents and recover more efficiently.	NanoLock offers prevention-based solutions.
Section II, Article 6, Clause 8 The ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives, by: (a) explaining how the ICT risk management framework supports the financial entity's business strategy and objectives; (b) establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analyzing the impact tolerance for ICT disruptions; (c) setting out clear information security objectives, including key performance indicators and key risk metrics; (d) explaining the ICT reference architecture and any changes needed to reach specific business objectives; (e) outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it; (f) evidencing the current digital operational resilience situation on the basis of the number of major ICT-related incidents reported and the effectiveness of preventive measures; (g) implementing digital operational resilience testing, in accordance with Chapter IV of this Regulation; (h) outlining a communication strategy in the event of ICT-related incidents the disclosure of which is required in accordance with Article 14.	NanoLock offers prevention-based solutions. It applies a zero-trust mechanism at the device level, ensuring that every access, change request, or update attempt through a PLC is always authenticated and authorized, regardless of its origin.

Requirements	The Nanolock Solution
Article 9 - Protection and prevention 2. Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit. 3. In order to achieve the objectives referred to in paragraph 2, financial entities shall use ICT solutions and processes that are appropriate in accordance with Article 4. Those ICT solutions and processes shall: (a) ensure the security of the means of transfer of data; (b) minimize the risk of corruption or loss of data, unauthorized access and technical flaws that may hinder business activity; (c) prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data; L 333/32 EN Official Journal of the European Union 27.12.2022; (d) ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error.	NanoLock significantly reduces the risk of corruption or loss of data, unauthorized access and change requests. It ensures operational integrity by protecting from human errors – whether they are in-house employees, outsourced contractors or other third parties.
4. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall: (c) implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof; (d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes; (e) implement documented policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner.	NanoLock limits access privileges based on predefined criteria. All change requests and update attempts are authenticated before being implemented.

NanoLock OT Defender - Solution Diagram