



# Addressing NIS2 Compliance with PAM

Prepare your organization for required security controls with **Securden Unified PAM**

---

**Whitepaper**



## Index

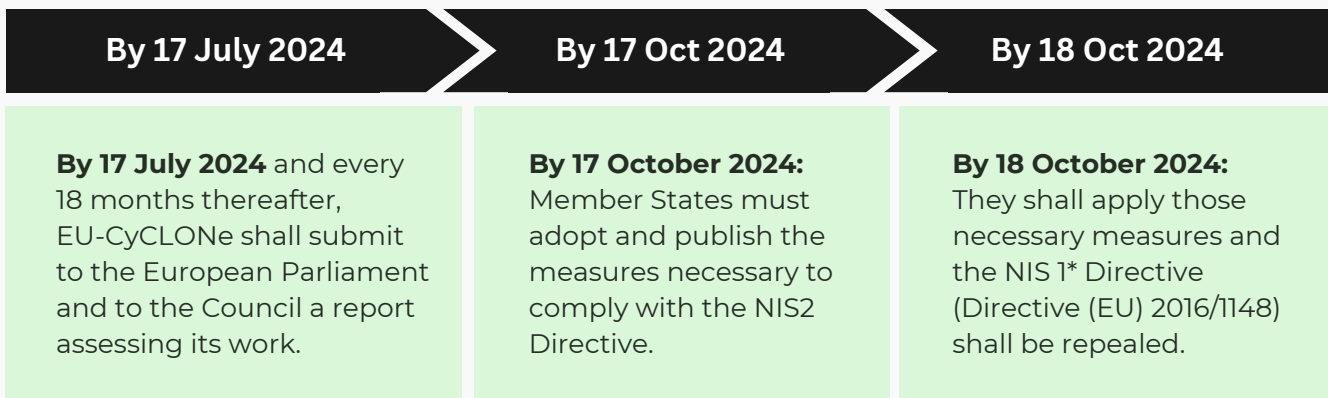
1. Introduction: What Is NIS2.....	03
2. What Has Changed With NIS2?.....	03
3. Who Does The NIS2 Directive Apply To?.....	04
4. Supporting Entities: EU-CyCLONe And CSIRT.....	06
5. The Main Objectives Of NIS2.....	07
6. How Your Business Can Prepare.....	09
7. Prepare For Expected Security Controls.....	10
8. How Securden Unified PAM Helps Comply With NIS2.....	14

## Introduction: What Is NIS2?



The NIS2 Directive ([EU-wide legislative act: Directive \(EU\) 2022/2555](#)) was released with the aim to achieve a higher level of cybersecurity for Networks and Information Systems (NIS) across entities that work with European member states.

### Adoption Timelines



## What Has Changed With NIS2?



The NIS2 directive came from a proposal to revise the NIS directive which was successfully adopted by the European Commission.

It came as a response to growing threats posed with digitization and from the surge of cyberattacks. The main objectives were to streamline reporting obligations, introduce supervisory measures that were more stringent and make enforcement requirements stricter.

## Key changes in the directive

The main differences between NIS and the newer NIS2 Directive are summarized:

- NIS2 eliminates the classification and distinction between operators of essential services (OES) and providers of digital services (DSP). Instead, the NIS2 provides different rules for "essential entities" and "important entities". DSPs have not disappeared from the list of target companies but have been redistributed among the list of essential and important entities.
- New sectors that were previously not in focus have been included in the NIS2 directive. These sectors are considered critical to the economy and public (e.g. postal & courier services, wastewater management, food, etc).
- Security requirements for supply chains and suppliers have been included and made stringent.
- The establishment of a European Cyber Crises Liaison Organization Network (EU-CyCLONe)
- Greater coordination is established in the disclosure of new vulnerabilities discovered throughout the Union and stricter supervisory measures for national authorities, stricter enforcement requirements and aims to harmonize sanctioning regimes across Member States.

NIS2 modernizes the existing (NIS) framework to keep up with the evolving cyberthreat landscape and increased digital adoption. With new sectors, it aims to improve the resilience of entities.

## Who Does The NIS2 Directive Apply To?

NIS2 applies to any organization providing critical services in an EU member country, NIS2 must be incorporated into the national laws of each EU member by 2024 October. These organizations are obligated to take appropriate measures as defined by the directive to manage and mitigate cyber risks and minimize the impact of incidents. The entities are classified as below.

## Classification of Critical Entities

if your organization falls under a critical category as defined below, NIS2 directives apply to you.

<b>Essential entities</b> Generally large organizations in highly critical sectors	<b>Important entities</b> Mid-sized and large organizations as specified by NIS2
<ul style="list-style-type: none"> <li>• <b>Energy</b> (electricity, oil and gas, covering production, storage and transmission activities - hydrogen as added by NIS2)</li> <li>• <b>Drinking water</b></li> <li>• <b>Wastewater</b> (collection, disposal or treatment of municipal wastewater, domestic wastewater or industrial wastewater)</li> <li>• <b>Transportation</b> (air, rail, water, road)</li> <li>• <b>Banking</b></li> <li>• <b>Financial markets</b></li> <li>• <b>Digital infrastructure</b> (Internet nodes; DNS service providers; TLD name registries; cloud computing service providers; data center service providers; content delivery networks; trust service providers; providers of public electronic communication networks and public electronic communication services)</li> <li>• <b>ICT service management</b> (managed service providers and managed security service providers)</li> <li>• <b>Governments</b> (central, as well as regional, the latter only risk-based, but excluding defense or national security and law enforcement, as well as the judiciary, parliaments, and central banks)</li> <li>• <b>Healthcare</b> (hospitals but under NIS now also includes reference laboratories, manufacturers of medical devices or pharmaceutical preparations and others)</li> <li>• <b>Space</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Postal and courier services</b></li> <li>• <b>Waste management</b></li> <li>• <b>Accounting firms</b></li> <li>• <b>Digital providers</b> (online marketplaces, online search engines and social networking platforms)</li> <li>• <b>Research organizations</b> (excluding education)</li> <li>• <b>Chemicals</b> (Production and distribution)</li> <li>• <b>Food</b> (Wholesale, industrial food production and processing)</li> <li>• <b>Manufacturing</b> (Medical devices, electrical equipment, motor vehicles, machinery and equipment)</li> </ul>

Medium and large companies from these sectors within the EU must now comply with NIS2. Smaller organizations could be included if they carry out critical functions.

While there is no difference in requirements between both these entities, essential entities will have to comply with supervision requirements from the introduction of NIS2, while important entities will be subject to ex-post supervision, meaning that action will be taken if authorities receive evidence of non-compliance.

## Supporting Entities: EU-CyCLONe And CSIRT



As part of the NIS2 initiative, certain entities have been established to help with cooperation.

### **The EU-CyCLONe**

As part of this initiative, the European cyber crisis liaison organization network (EU-CyCLONe) was established. The EU-CyCLONe supports the coordinated management of large-scale cybersecurity incidents to ensure the regular exchange of information among member states, union institutions, bodies, offices and agencies.

### **NIS Cooperation Group and CSIRT Responsibilities**

The NIS Cooperation Group functions according to the European Commission and follows its own rules of procedure. On the operational side, the NIS Cooperation Group is supported by the work of the network of Computer Security Incident Response Teams (CSIRTs), dedicated to sharing information about risks and ongoing threats, and cooperating on specific cybersecurity incidents. The NIS Cooperation Group provides strategic guidance for the activities of the CSIRTs network.

These entities ensure that organizations meet the objectives of NIS2.

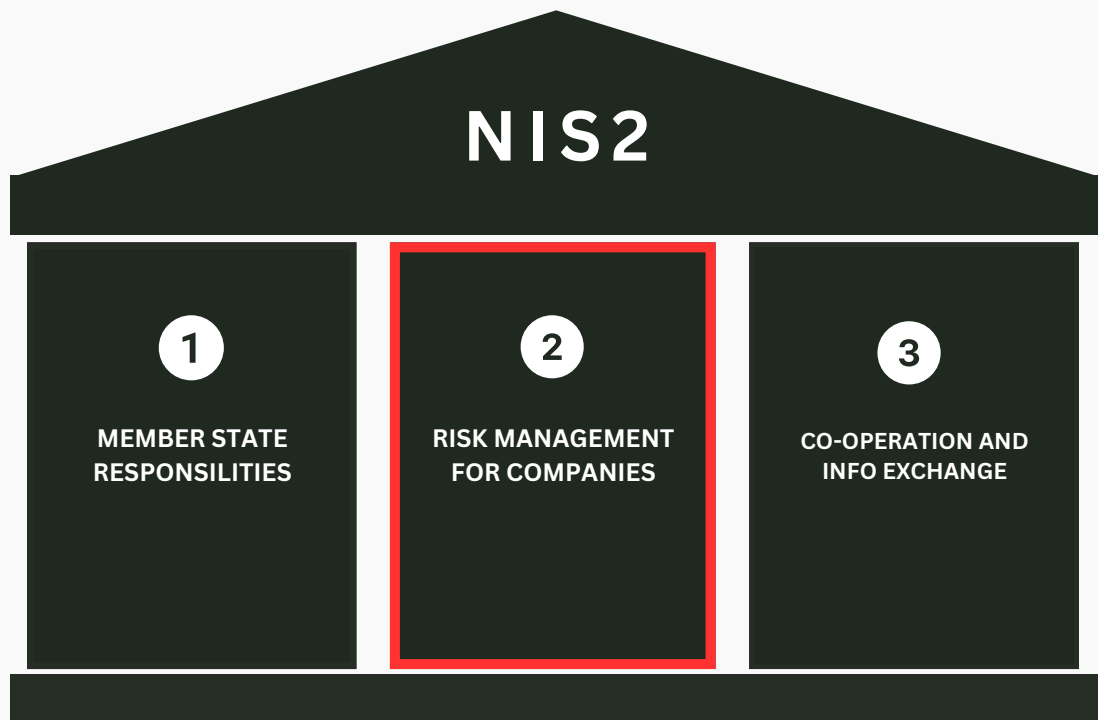
# The Main Objectives Of NIS2

## Three Main Pillars of NIS2

The primary objectives of NIS2 can be divided into three categories:

- 1 Responsibilities of member states
- 2 Information exchange and cooperation with the govt
- 3 Risk management and security measures to be taken by companies

This whitepaper / handbook will focus on the security measures that organizations are required to take and how a PAM solution can help comply with a number of NIS2 requirements.



## Repercussions of not meeting obligations

A minimum set of administrative sanctions has been established in case organizations do not follow the obligations set in the NIS2 directive.

### Administrative fines:

#### For essential entities:

Administrative fines of up to **10,000,000 euros** or at least 2% of the total annual global turnover in the previous fiscal year of the company to which the essential entity belongs, whichever amount is higher.

#### For important entities:

Administrative fines of up to **7,000,000 euros** or at least 1.4% of the total annual global turnover in the previous fiscal year of the company to which the key entity belongs, whichever is higher.

All important and essential entities must notify about incidents that are 'severe'. Local government, authorities, and CSIRT support and information sharing across entities are one of the main areas of regulation.

### An incident shall be considered to be significant if:

- It causes or may cause severe operational disruption of the services or financial loss for the entity concerned.
- It affects or may affect other natural or legal persons by causing considerable material or non-material damage.

Precise provisions are introduced on reporting incidents, the report content and timing. Reporting must now be done within 24 hours of the discovery of the incident – (Instead of 72 hours previously)



## C-Level Management Now Accountable

To reduce the pressure that falls on the IT team personnel to maintain security across the organization, new measures have been introduced to hold C-level management responsible. NIS2 holds top level managers personally liable if gross negligence is proven after a cyber incident. The measures to be taken include:

- Ordering public announcement of compliance violations.
- Identifying person(s) responsible for any violation and give a public statement.
- Banning (temporarily) the identified individual from having a management role when violations are repeated.

## How Your Business Can Prepare



While preparing for NIS2 can be tasking for large and small organizations alike, a step-by-step approach with proper roadmaps and planning can help with satisfying security requirements.

### Review existing security controls

Go over the current security posture of your organization, assess risks based on your infrastructure, access controls and sensitive assets/data. Review incident detection and response management capabilities and define local/regional (EU)/global responsibilities.

### Fill in any security gaps

Identify solutions that can help fill your IT security gaps, especially when it comes to data security. Look for solutions that can address security gaps, increase efficiency and operate at a reasonable cost. The solution must also be able to scale with growth in your organization.


# Prepare For Expected Security Controls




Privileged Access Management (PAM) solutions help to address directive requirements in the segments of Access Control, Basic Cyber (Password) Hygiene, Zero Trust Policies, Supply Chain Security, Cryptography, and Encryption Tools.


## Addressing NIS2 directives with Securden Unified PAM


A mapping of NIS2 requirements to global security standards has been released by ENISA. We have mapped major security controls that can be satisfied by Securden Unified PAM.

NIS Directory Requirements / NIS2 Obligations	Requirement Summary	 How Securden Unified PAM Helps
Incident Reporting		
<p><b>NIS Directory Paragraph 23 – Incident Reporting</b></p>	<p>Entities must ensure that there are measures in place to notify risks about significant incidents.</p> <p>Comprehensive details about incidents would be required for submitting to the authorities via reports.</p>	<p>Securden Unified PAM acts as the central repository for all devices in the organization as well as their accounts. All access to these sensitive resources is carried out through it.</p> <p>Major cybersecurity incidents occur due to credential leakage or through gaining access to these sensitive resources.</p> <p>With all privileged activities being routed securely through <b>Securden Unified PAM</b>, comprehensive auditing and notification capabilities help notify the administrator and other concerned authorities if any incident takes place.</p>

<p>NIS Directory Requirements / NIS2 Obligations</p>	<p>Requirement Summary</p>	<p> How Securden Unified PAM Helps</p>
<p><b>Incident Reporting</b></p>		
<p><b>NIS Directory Paragraph 102 - Incident Timelines</b></p>	<p>When entities become aware of a significant incident, they should submit an early warning without undue delay and in any event within 24 hours.</p> <p>That early warning should be followed by an incident notification. The entities concerned should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident.</p> <p>A final report within one month of their handling of the significant incident.</p>	<p>Comprehensive reports, audit trails and recordings of all privileged sessions provide documentation for incidents and cyber-attacks.</p> <p>Endpoint privilege security helps notify incidents related to Windows security events.</p> <p>Reports can be generated periodically depicting all critical activity. These reports will be readily available to notify authorities within required timelines.</p>
<p><b>Cyber Hygiene</b></p>		
<p><b>NIS Directory Paragraph 49 - Maintain Cyber Hygiene for Infrastructure</b></p>	<p>Entities must maintain cyber hygiene and protect all business and end-user data.</p> <p>Cyber hygiene policies comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installs, the limitation of administrator-level access accounts, and the backing-up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or cyber threats.</p>	<p><b>Securden Unified PAM</b> helps set a baseline standard by helping define policies for password length, strength, frequency of rotation and more.</p> <p>Access controls ensure that users can only gain access to the passwords and accounts shared to them through <b>Securden Unified PAM</b>.</p> <p>With the PEDM module, all administrative accounts can be eliminated to prevent privilege escalation. For new installations, software updates, admin access, and access to applications comprehensive control policies can be defined.</p>

<p>NIS Directory Requirements / NIS2 Obligations</p>	<p>Requirement Summary</p>	<p> How Securden Unified PAM Helps</p>
<p><b>NIS Directory Paragraph 89 - Cyber Hygiene for Users</b></p>	<p>Good cyber hygiene practices must be in place for users such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management.</p>	<p>MFA and SSO help authenticate users and maintain zero-trust when accessing privileged resources through Securden Unified PAM.</p> <p>Dark web monitoring and password analysis capabilities inform users if they have weak/breached passwords in use and prompts them to generate a strong password and use that instead.</p> <p>Just in time access ensures that users can only have time-restricted windowed access to resources and supports zero-trust principles.</p>
<p>Network Security</p>		
<p><b>NIS Directory Paragraph 43 - Proactive Network Scanning</b></p>	<p>Entities must have proactive network scanning capabilities to gather the information systems used for their services.</p>	<p>Securden Unified PAM helps scan distributed networks and identify all privileged systems and accounts within them.</p>
<p><b>NIS Directory Paragraph 53 - Protect Connected Networks in the Utility Sector</b></p>	<p>Protect the utility sector against threats and mitigate attacks in interconnected networks.</p>	<p>Securden Unified PAM mitigates attacks by managing sensitive credentials (to prevent credential phishing), isolating privileged sessions, enabling just-in-time access to resources and enforcing Zero standing privileges.</p> <p>Endpoint privilege management capabilities ensure that the local admin account cannot be exploited to launch cyberattacks and escalate across the network.</p>

NIS Directory Requirements / NIS2 Obligations	Requirement Summary	 How Securden Unified PAM Helps
Ransomware defense, risk management and supply chain security		
<p><b>NIS Directory Paragraph 54 - Address Ransomware Attacks</b></p>	<p>Defend infrastructure against ransomware attacks and different attack patterns.</p>	<p>Securden Unified PAM has endpoint privilege management capabilities that help defend against ransomware by eliminating the local admin rights on all endpoints in the infrastructure. Access to applications is granted based on control policies and admin approval.</p> <p>Securden Unified PAM controls for remote sessions ensure that privileged sessions can only be launched by authorized users and all activity is monitored, recorded and audited comprehensively.</p>
<p><b>NIS Directory Paragraph 77 - Risk assessments and risk management</b></p>	<p>Risk management measures must be put in place to ensure the security of the network and information systems. Risk assessments must be carried out and appropriate measures must be taken.</p>	<p>A major driver for cyberattacks is weak passwords, or passwords that have been leaked in previous data breaches.</p> <p>Securden Unified PAM scans your network and identifies all privileged passwords – which are then analyzed and given a risk score.</p> <p>These weak passwords can be replaced by generating strong passwords.</p> <p>Additionally, all credentials that have been leaked in the dark web can be identified and changed.</p>
<p><b>NIS Directory Paragraph 85 - Protect the supply chain against vulnerabilities.</b></p>	<p>Entities should assess and consider the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and</p>	<p>Password and credential management form the core of Securden Unified PAM and reduce the risk of supply chain attacks with the use of strong credentials across the environment that are constantly rotated.</p>

NIS Directory Requirements / NIS2 Obligations	Requirement Summary	 How Securden Unified PAM Helps
	incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers.	Through API capabilities, hardcoded passwords can be eliminated, and application passwords can be fetched securely.
<b>Encryption</b>		
<b>NIS Directory Paragraph 98 - Encryption and Datacentric security for Public Electronic Communications.</b>	The use of encryption technologies, in particular end-to-end encryption as well as datacentric security concepts, such as cartography, segmentation, tagging, access policy and access management, and automated access decisions, should be promoted.	<p><b>Securden Unified PAM</b> encrypts all sensitive data like privileged credentials end-to-end, while in rest, as well as in transit.</p> <p>Access control policies can ensure users only have access to the resources they need. Endpoint privilege management helps with just in time elevation of privileges.</p>

## How Securden Unified PAM Helps Comply With NIS2



Securden Unified PAM has the capabilities to secure all sensitive data and protect access to resources used by critical entities. Regulations and mandates as per the NIS2 directive can be met through comprehensive access controls, customizable reports and auditing mechanisms, privilege management of endpoint systems and management of privileged remote sessions.

Important and essential entities can leverage these capabilities whether they operate on-prem, on cloud or have a hybrid distributed environment.