

# NIS/NIS2 DIRECTIVES

Privileged Access Management,  
a Key Element in NIS/NIS2 Compliance



# NIS/NIS2 DIRECTIVES

## Privileged Access Management, a Key Element in NIS/NIS2 Compliance

### SUMMARY

Adopted on July 6, 2016, the NIS (Network Infrastructure Security) Directive was transposed by the European Union Member States on May 9, 2018. This guideline has helped to homogenize the long national security practices of Member States, as well as to strengthen the protection of Operators of Essential Services (OESs) and Digital Service Providers (DSPs) against cyber threats.

In view of the technological developments and the consequences of the health crisis, the European Commission decided to update this NIS Directive by presenting a new proposal on December 16, 2020, "the NIS2 Directive".

In response to the growing threats posed by digitization and the increase of cyberattacks, this proposal aims to replace the NIS Directive and thereby strengthen security requirements, address the issue of supply chain security, streamline reporting obligations, and introduce stricter monitoring measures and enforcement requirements, including harmonized sanctions across the EU. After 17 months of discussions, the NIS2 Directive was agreed in a trilogue on May 13, 2022. The text, provisional at this stage, still needs to be finalized at the technical and linguistic levels before being formally adopted by the EU Council and the European Parliament. However, it already establishes a new scope of business sectors affected by cybersecurity regulations that will improve the resilience of the entire ecosystem. From now on, this ecosystem will be grouped around Essential Entities (EEs) and Important Entities (IE), including public administrations.

This white paper explains the impact of the revised NIS Directive - also known as the NIS2 Directive - on the cybersecurity practices of critical or important European entities and demonstrates how privileged access, endpoint, and identity management solutions can already help them comply

## INTRODUCTION

### What is the NIS Directive?

### What are the Changes Brought by the NIS2?

In the digital age, most companies and public organizations are digitizing and automating their information storage and handling processes, in particular to achieve economies of scale and gain in productivity and efficiency. The strong growth of digital technology in the daily lives of companies and individuals increases the market value of data tenfold and even enhances the value of certain critical resources, such as operators defined as providing an essential service (Essential Entities or EEs) or an important service (Important Entities or IEs). These entities are prime targets for hackers, increasing the risk of cyberattacks on organizations and individuals at several levels: financial/economic, reputational, or vital. Consequently, these companies or administrations must take all the necessary security measures to protect and arm themselves against cyberattacks.

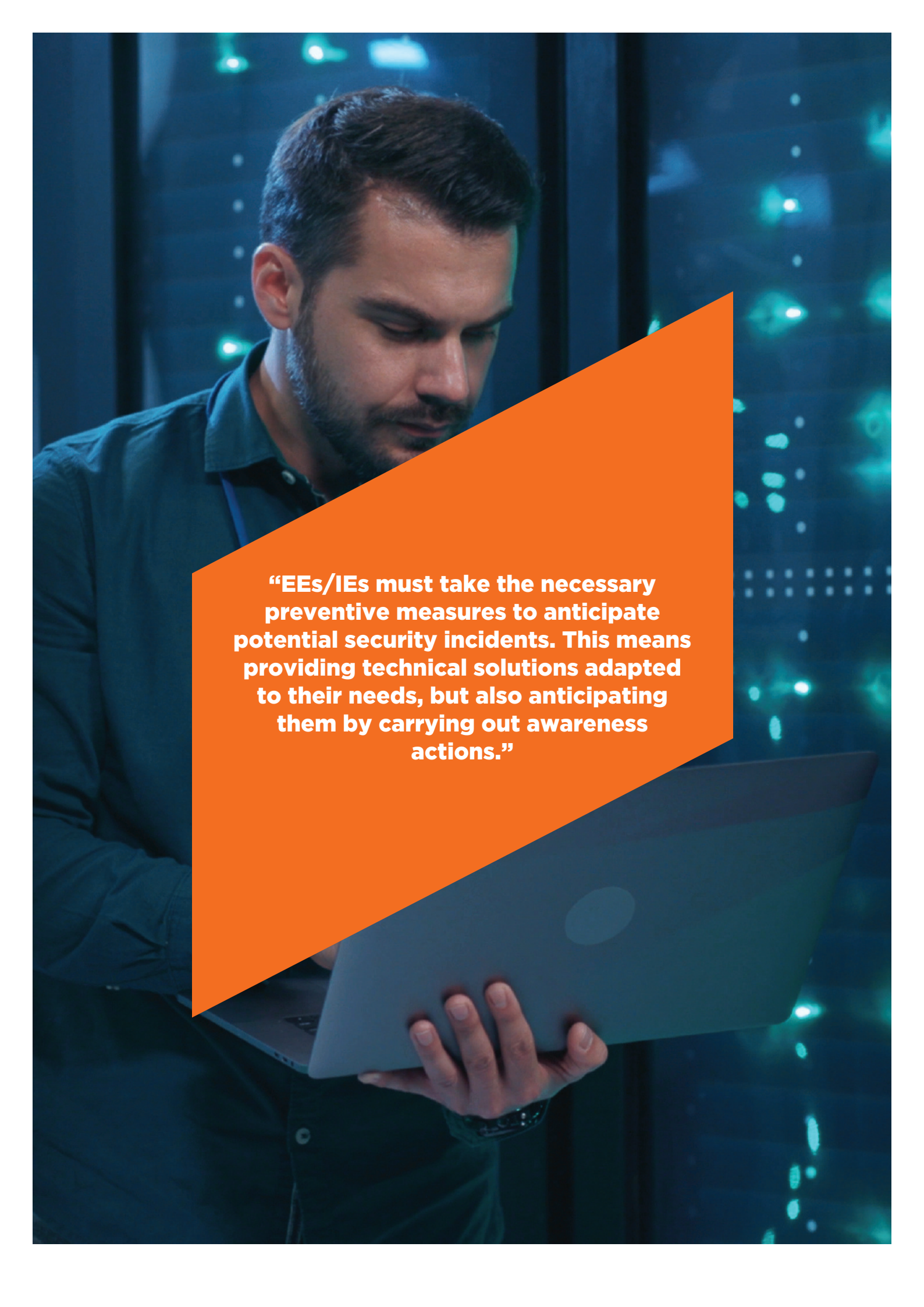
Furthermore, given the interconnectivity of systems and data within the European Union, it is also necessary to reinforce and extend a minimum level of security common to the various companies and organizations of the Member States. As attacks know no borders, this homogeneity is essential to the overall stability and security of the EU, which depends on that of each of its Member States.

The NIS Directive provides, as of 2018, a common legal framework for all Member States to strengthen security and ensure the stability of the EU in the face of cyber threats. It has made it possible to reinforce the cyber resilience of networks and IT systems of so-called critical infrastructures.

The currently under development NIS2 Directive will expand the scope of the existing NIS Directive by:

- defining new **Essential Entities (EEs)**,
- adding a level of **Important Operators (IEs)**, and
- including public administrations.

As a result, all these players will now have to report incidents affecting their networks and IT systems and submit, if necessary, to controls carried out by national regulatory authorities. They can therefore anticipate and identify the risks that threaten the security of their IT systems to take the appropriate measures to protect them. And for some, this will be a real structuring transformation.

A man with a beard, wearing a dark blue button-down shirt, is looking down at a silver laptop he is holding. The background is a server room with blue lighting and blurred server racks. An orange diagonal shape is overlaid on the image, containing white text.

**“EEs/IEs must take the necessary preventive measures to anticipate potential security incidents. This means providing technical solutions adapted to their needs, but also anticipating them by carrying out awareness actions.”**

In case of non-compliance or breaches, financial penalties can still be imposed and will be even intensified by this new directive.

From now on, the NIS2 Directive will require the Member States to strengthen sanctions in the event EEs and IEs, including Digital Service Providers (previously classified as DSPs) and administrations, violate their obligations. These sanctions will be administrative fines, the maximum amount of which may not be less than a certain threshold (Article 31):

- **For EEs:** up to 10 million euros or 2% of the entire global turnover.
- **For EEs and IEs,** in case of failure to comply with the obligations of Articles 18 (cyber risk management) and 20 (reporting): up to €7 million or 1.4% of the entire global turnover.

## Who is Affected?

To cover most of the risks faced by the EU on a daily basis, the NIS Directive as a whole focuses on three strategic targets:

- **The Essential Entities (or EEs)**, which replace the Operators of Essential Services (OESs) of the NIS Directive. These entities are those whose activity is vital not only to the national balance of the countries concerned, but also, and by default, for that of the EU. Until now, EEs belonged to various key sectors of activity, such as energy, banking, transport, healthcare, drinking water supply and distribution, digital infrastructures, and financial market infrastructures.

In addition to these 7 sectors initially included in the 2016 text, other industries have been added to Annex I of the future NIS2 Directive, including:

- Hydrogen
- Wastewater
- Some digital infrastructures (data centers, content providers, electronic communication providers, or cloud services)
- Space
- Public administrations, whose inclusion in the scope of the NIS2 Directive was particularly debated. In the end, only central governments would become EEs, the list of regional and local governments being left to the discretion of the Member States

- **The Important Entities (or IEs)** in the NIS2 Directive are operators recognized as indispensable for nations. They are acknowledged as complementary to EEs.

Under this name, Annex II of the NIS2 Directive refers today:

- Industrial production
- Chemical products
- Food
- Manufacturers and postal services
- Waste management sector

Furthermore, although this new directive expressly excludes micro-enterprises, it does apply to those that fall under Annexes I and II (defining essential or important services) and that fall into one of the following categories:

- Companies whose services are provided by an electronic communication network or an online public communication service, a trusted third party or a domain name service.
- Those whose entity is the sole provider of a service in a Member State or is particularly important at a regional, or national level.
- Entities for which the disruption of the service provided would have an impact on public safety and/or health or could induce systemic risks.
- Organizations identified as critical infrastructure in the sense of the directive on the resilience of critical entities (also known as "CER Directive"), which establishes close synergies with the proposed NIS2 Directive to cover the offline world.

- It is therefore understood here that Digital Service Providers (DSPs), which govern data storage and exchange of data on the Internet, will disappear as a separate category in the NIS2 Directive. They will be attached to the first two groups. Indeed, the new directive removes the distinction made between EEs and DSPs.

For all these players, the new status of **Essential Entity (EE)** or **Important Entity (IE)** will entail a real transformation linked to the implementation of specific technical and organizational security measures described in the NIS2 Directive to reinforce the protection of critical equipment and manage the risks threatening the security of their networks. Thousands of companies will now be obliged by law to raise the level of their IT security.

Finally, the NIS2 Directive will also clarify the relationship with other texts. Indeed, provisions have been introduced to clarify interactions with sectoral legislation, such as the DORA (Digital Operational Resilience Act) regulation on financial services and the CER Directive on the resilience of critical entities.

## Security Challenges

In addition to the organizational requirements to be implemented in the framework of NIS and NIS2, Member States rely on the competent authorities or their Computer Security Incident Response Teams (CSIRTs) to ensure compliance with the security rules specific to their Essential and Important Entities.

### **The Challenges of Essential Entities and Important Entities**

The NIS and NIS2 directives provide for the adoption of security measures to ensure the protection and compliance of EE/IEs. Specifically, they must ensure the definition and implementation of technical and organizational security measures proportionate to the risks to which they are exposed. This implies being aware of the dangers and how they evolve as new technologies and IT practices emerge. The directive encourages this awareness by requiring OEs to regularly assess their cybersecurity risks.

EEs/IEs must also take preventive measures to anticipate potential security incidents. This means having technical solutions adapted to their needs, but also anticipating these incidents by carrying out awareness-raising actions to reduce the risks of negligence or informing stakeholders of good security practices and their role in securing each entity.

The proposal includes a list of seven key elements that all companies must address or implement as part of their actions, including incident response, supply chain security, encryption, and vulnerability disclosure.

Furthermore, the text provides a two-step approach to incident reporting. Affected companies have 24 hours from the time they become aware of an incident to submit an initial report, followed by a final report no later than one month later.

These proposed new communication rules will improve the way the EU prevents, handles, and responds to large-scale cybersecurity incidents and crises by introducing clear responsibilities, proper planning, and greater EU cooperation. The revised directive would establish a European crisis management system (EU CyCLONe) to support the coordinated management of cybersecurity incidents at the EU level, as well as to ensure regular information exchange.

## **New Challenges for Administrations**

These challenges no longer only affect private operators. With the increasing dematerialization of data and the multiplication of digital tools, cybersecurity has become an issue of national sovereignty. The risk of cyberattacks has increased with the lockdown that has forced many government employees to telecommute. However, remote work has been developed in a hurry, most of the time without an adapted security framework. The proliferation of connected personal computers is a potential gateway to the local authority's IT system.

The challenge of protecting against cyber risks is therefore becoming increasingly important for administrations, especially since the protection of citizens' data – patients in the case of public hospitals and agents in the case of government entities managing territorial security - remains a major concern for IT departments.

Expectations for compliance with the NIS2 Directive will consequently be extremely high.

But beyond the issue of integrating central and local governments, it should be noted that the new text will apply to several important sectors related to public authorities: wastewater treatment, drinking water supply, and waste management. While private companies specializing in these areas will have to meet new obligations, it would be surprising if public authorities were to escape them.

These are new challenges that all administrations will have to consider today to meet the NIS2 expectations in the coming months.

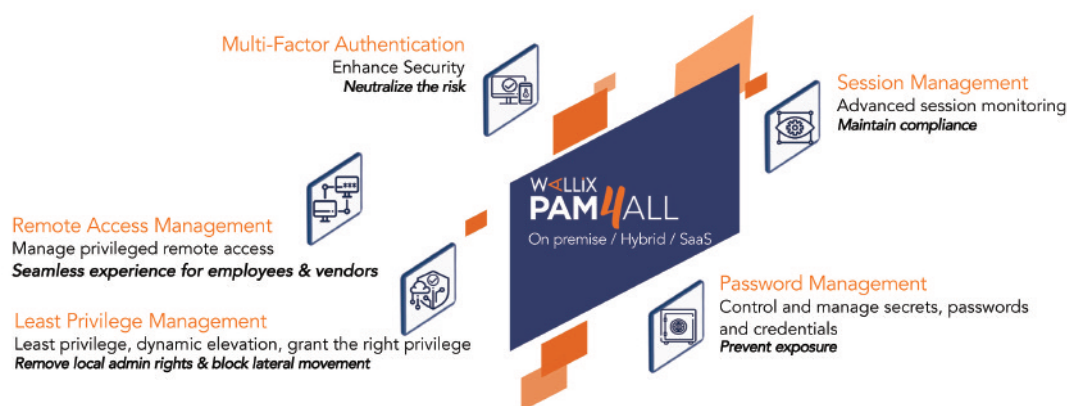


## The Role of Identity and Privilege Management in NIS/NIS2 Compliance

Fine-grained identity and access management helps to effectively address many of the organizational and technical issues outlined by the NIS and NIS2 directives.

This is a key compliance component of both directives, and it requires the implementation and monitoring of state-of-the-art security practices, including requiring organizations subject to the directive to define a stable and scalable security policy, and to implement advanced prevention, detection, response, and compliance measures.

There are a few quick and effective steps that can be implemented quickly to align with these recommendations, including:



## Strengthening Identity Management and Authenticating Users

NIS2 does not deviate from the standard already set by the NIS Directive to put in place all the tools to prevent a cybercriminal from accessing an organization's databases and data. Authentication of employee identities through secure access to strategic applications and data is therefore a crucial first step in strengthening the security policy of entities affected by NIS2.

The three-step security process (identification, authentication, authorization) must be applied to the IT infrastructure to ensure that individuals accessing resources are who they claim to be and that they have the authority to access sensitive data of essential or important organizations.

## Identification

The NIS and NIS2 directives recommend being able to attribute any action performed on an IT system to a user or an automatic process, by associating an identity to each person or process, and then an identity to each action performed.

Identity is, in fact, the starting point for access security. Given the amount of sensitive data stored in the EE/IEs' IT infrastructure, it is essential to be able to distinguish digital users with the same degree of accuracy as physical identities.

Users are given unique credentials and are known by their personal identification information, username, and password.

And simple credentials alone are not enough to keep a network secure, as they leave the system vulnerable to dishonest users claiming someone else's identity. They must be backed up with strong authentication.

## Authentication

The NIS/NIS2 directives require the operator to protect access to its sensitive resources, whether by a user or by an automated process, by means of an authentication mechanism that includes at least one secret element. Authentication is, in effect, the stage in the security process where a user must prove his or her claimed identity. Authentication prior to authorization of access to resources follows the "Zero Trust" model of cybersecurity. Zero Trust means that identity and privileges are never assumed, and they must always be verified through strict security protocols.

This authentication can be strengthened by using two-factor authentication: several types of authentication factors allow a user's identity to be validated by different and complementary sources.

## Controlling Access Permissions Using the Principle of Least Privilege

Once the user has been authenticated, the authorizations given to him answer this last question of the access security process posed by the NIS and NIS2 directives. The entity must define the rules for managing and assigning access rights to its resources, in accordance with its IT systems security policy. Indeed, weak authorization can lead to the risk of privileged users accidentally or deliberately abusing their privileges.

A company or an administration can then be exposed to risks of fraud, data theft, and reputational damage.

EE/IEs should assign to a user or automatic process only those rights that are strictly necessary to perform the actions that are proven to be useful. The NIS/NIS2 directives recommend that no rights be assigned to a user or automatic process by default. For each access need, the following questions should be asked: Does the user need access to the application? What level of access is needed to perform the task? And for how long will the access be needed? As a result, it is essential to finally manage the rights at the application and process level.

EPM (or Endpoint Privilege Management) solutions address this need for elevated privileges on user accounts through innovative permissions management for all users.

They ensure that controlled authorizations are in place at the process and application levels. They eliminate privileged accounts and local administrative rights. In doing so, EPM solutions help contain the privileges of potentially dangerous applications (email clients, browsers, etc. with Internet access) by denying access to sensitive resources, regardless of the user's privilege level. They prevent malware, ransomware, and cryptovirus from executing or encrypting files. Finally, EPM solutions put an end to shared passwords being used on countless devices and tools through local administrator accounts.

## Securing Privileged Accounts

A special case mentioned by the NIS/NIS2 directives is the detailed assignment of access rights for privileged accounts. Indeed, within organizations, privileged users have high administrative rights. They can therefore represent a significant threat to EEs and IEs. They are particularly sensitive and consequently require special traceability.

EE/IEs need to implement a robust Privileged Access Management (PAM) solution to ensure that only authorized users can access sensitive resources at the right times. This allows IT administrators to centrally manage target users and systems, and then set rules and authorization conditions to automatically grant or deny access to critical resources. They can also monitor and record the actions of privileged users during a session for auditing purposes or to stop any suspicious activity in real-time for both internal users and external providers and suppliers.

PAM (or Privileged Access Management) protects confidential and strategic data from cyberattacks by controlling access to target systems and the actions of their users. These privileged users often have one or more access to sensitive digital data. Whether granted legitimately, negligently, or via an attack that allows them to elevate privileges, these accesses present a significant risk to operators subject to the NIS/NIS2 directives. A careless or malicious privileged user can steal data, compromise its integrity, or delete it, causing a serious security incident.

For all EEs/IEs, it is therefore imperative to:

- Secure confidential data by controlling access to the most critical resources.
- Prevent exposure by managing secrets and passwords.
- Gain complete visibility into the activities perpetrated by privileged users by identifying who has access to what when, how, and why.
- Maintain compliance through advanced session monitoring.

These aspects are key components ensure compliance with the NIS and NIS2 directives through the implementation and monitoring of the latest security practices, including requiring organizations subject to the directive to define a stable and scalable security policy and to implement advanced prevention, detection, response, and compliance measures.

## Conclusion

To protect so-called essential or important services and strengthen the stability of the European Union in the face of cyber threats, the NIS and future NIS2 directives continue to impose minimum security practices on Essential and Important Entities in each Member State, extending to public administrations. The proposal details a legislative framework that implies a significant upgrade in cybersecurity, particularly in areas related to monitoring and enforcement.

Sectors previously considered outside the scope of NIS and cybersecurity in general, are now within the scope, due to their critical role in the broader economy and the proliferation of digital technologies expanding the attack surface for malicious actors.

Identity Management (IM), Endpoint Management (EPM), and Privileged Access Management (PAM) clearly help organizations in the Member States to meet the compliance challenges posed by these two directives by supporting them in defining a security policy and reinforcing incident prevention, detection, and reporting practices. By combining management, control, and traceability with ease of deployment and integration, IM, EPM, and PAM solutions are key elements of the digital chain of trust that contribute to meeting the security challenges of the NIS Directive as it is defined today and will also ensure compliance with the expansion advocated by the future NIS2 Directive.

## About WALLIX

A software company providing cybersecurity solutions, WALLIX is the European specialist in digital Identity and Access Security Solutions. WALLIX's technologies enable companies to respond to today's data protection challenges. They guarantee detection of and resilience to cyberattacks, which enables business continuity. They also ensure compliance with regulatory requirements regarding access to IT infrastructures and critical data. WALLIX has a strong distribution network of more than 300 resellers and integrators worldwide. Listed on the Euronext (ALLIX), WALLIX supports more than 2000 organizations in securing their digital transformation.

WALLIX affirms its digital responsibility and is committed to contributing to the construction of a trusted European digital space, guaranteeing the security and confidentiality of data for organizations as well as for individuals concerned about the protection of their digital identity and privacy.

[WWW.WALLIX.COM](http://WWW.WALLIX.COM)



**WALLIX**  
CYBERSECURITY SIMPLIFIED