

White Paper

# Network and Information Security Directive 2 (NIS2)

Help your organization comply with the European Union's NIS2 Directive with Thales

[cpl.thalesgroup.com](https://cpl.thalesgroup.com)

**THALES**  
Building a future we can all trust

## Introduction

The European Union's Network and Information Security Directive (NIS) is a legislative act that aims to achieve a high common level of cybersecurity for organizations across the European Union. Originally adopted in 2016, NIS relied heavily on the discretion of individual member states and lacked accountability.

On January 16, 2023, in response to growing threats posed by increasing digitalization and the surge in cyber-attacks, the EU adopted NIS2 to strengthen security requirements and cyber resilience. The EU's 27 Member States have until October 17, 2024, to transpose the NIS2 Directive into applicable, national laws.

NIS2 requires operators of critical infrastructure and essential services in the EU to implement appropriate security measures and report any incident to the relevant authorities. The Directive addresses the security of supply chains, streamlines reporting obligations, and introduces more stringent supervisory measures and stricter enforcement requirements, including harmonized sanctions across the EU.

A critical cybersecurity strategy for any organization is protecting sensitive data, access, identities, applications, and systems essential for its operations. This paper outlines how Thales can help meet the demands of NIS2.

## Evolving from NIS to NIS2

NIS2 expands the original NIS Directive to cover more industry sectors, with additional risk-management measures and incident reporting obligations. It also provides for stronger enforcement. NIS2 adds to NIS in 4 key areas:

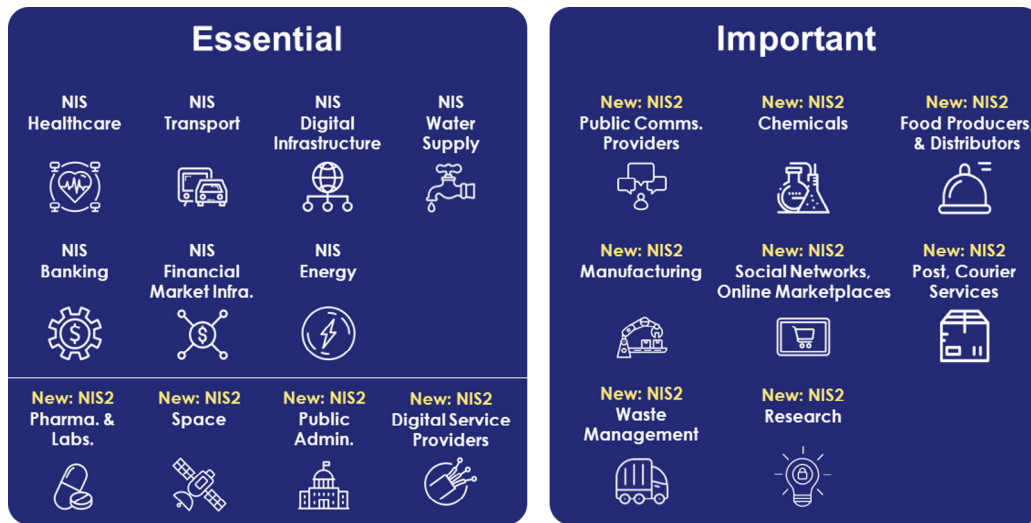
- **Expanded scope:** NIS2 extends its reach from seven to eighteen sectors. NIS2 has also categorized each sector as essential or important, with different supervision requirements.
- **More stringent security requirements:** The Directive enforces stricter cybersecurity measures. These requirements involve risk management practices, technical and organizational measures, incident response and recovery plans, employee training, and frequent updates and patching.
- **Mandatory incident reporting with specific timeframes:** NIS2 requires organizations to report significant cybersecurity incidents, which are those that are likely to adversely affect the provision of the organization's services. Organizations must provide an "early warning" report, using a standardized format and a shortened reporting timeframe of 24 hours, followed by an Incident Notification within 72-hours of first becoming aware of the incident, as well as a Final Report within 30 days.
- **Enforcement through penalties:** The NIS2 Directive imposes more severe penalties for non-compliance, including increased financial penalties.

### Expanded Scope: Essential vs. Important Entities

NIS2 has expanded the directive's scope from seven sectors to eighteen. The previous version of NIS identified healthcare, transport, digital infrastructure, water supply, banking, financial market infrastructure, and energy as essential sectors. NIS2 adds digital service providers, pharmaceutical and labs, space, and public administration to the 'Essential' sectors category. NIS2 also adds an 'Important' sector category, including public communications providers, chemicals, food producers and distributors, critical device manufacturers, social network and online marketplaces, courier services, research, and waste management.

Figure 1 below shows the original NIS sectors and the expanded NIS2 sectors along with the designation of essential or important. The major difference between the two categorizations is how the entities are supervised.

Figure 1



Essential entities must comply with supervision requirements, while important entities will only be subject to ex-post supervision. Ex-post supervision means that supervision action will be taken only if authorities receive evidence of non-compliance.

Individual member states can determine what constitutes supervision, such as:

- On-site inspections and off-site surveillance, including random checks and regular audits.
- Targeted security audits on risk assessments or risk-related available information.
- Safety scans are based on objective, non-discriminatory, fair, and transparent risk assessment criteria.
- Request for information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies.
- Requests for access to data, documents, or information necessary for performing their supervisory tasks.
- Requests for evidence of the implementation of cybersecurity policy, such as the results of security audits conducted by a qualified auditor and the respective underlying evidence.

## More Stringent Security Requirements

Article 21 of NIS2 states, “Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational, and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or the provision of their services and to prevent or minimize the impact of incidents on recipients of their services and on other services.” The goal of Article 21 is to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following:

- a. policies on risk analysis and information system security;
- b. incident handling;
- c. business continuity, such as backup management, disaster recovery, and crisis management;
- d. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- e. security in the network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure;
- f. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- g. basic cyber hygiene practices and cybersecurity training;
- h. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- i. human resources security, access control policies, and asset management;
- j. the use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems within the entity, where appropriate.

## Mandatory Timeframes for Reporting

Article 23 of NIS2 requires that every significant cybersecurity incident “...that has a significant impact on the provision of their services...” be reported, whether or not the attack actually affected the entity’s operations. The purpose of this is to help authorities improve monitoring and responses to potential threats. NIS2 maintains the requirement from NIS that every EU member state designates a central point of contact for compliance and a coordinating Computer Security Incident Response Team (CSIRT) for incident reporting or a competent authority.

The most significant change around incident reporting is how the NIS2 Directive details the mandatory multi-stage incident reporting process and the content that must be included.

### **Early Warning: Within 24 hours.**

An initial report must be submitted to the competent authority or the nationally relevant CSIRT within 24 hours of a cybersecurity incident. The initial report should provide an early warning where there may be cross-border impact or maliciousness involved. This first notification is intended to limit the potential spread of a cyber threat.

### **Follow-up Incident Notification: Within 72 Hours.**

A more detailed notification report must be communicated within 72 hours. It should contain an assessment of the incident, including its severity, impact, and indicators of compromise. The impacted entity should also report the incident to law enforcement authorities if it was criminal.

### **Final report: Within one month.**

A final report must be submitted within one month after the initial notification or first report. This final report must include:

- A detailed description of the incident.
- The severity and consequences.
- The type of threat or cause likely to have led to the incident.
- All applied and ongoing mitigation measures.

Additionally, under the NIS2 Directive, entities must report any major cyber threat they identify that could result in a significant incident. A threat is considered significant if it results in:

- Material operational disruption or financial losses for the entity concerned.
- It may affect natural or legal persons by causing significant material or immaterial damage.

## Enforcement Through Penalties: Failure to Comply.

Failure to comply with the NIS2 Directive comes with stricter penalties than NIS. Under the NIS2 Directive, penalties for non-compliance differ for essential entities and important entities.

- For essential entities, administrative fines can be up to €10,000,000 or at least 2% of the total annual worldwide turnover in the previous fiscal year of the company to which the essential entity belongs, whichever amount is higher.
- For important entities, administrative fines can be up to €7,000,000 or at least 1.4% of the total annual worldwide turnover in the previous fiscal year of the company to which the important entity belongs, whichever amount is higher.

## How Thales Helps with NIS2 Compliance

Thales can help Essential and Important entities comply with NIS2 by addressing essential cybersecurity risk-management requirements under article 21 and by helping organizations produce complete, accurate, and timely reports to meet article 23 requirements. We provide solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

- **Application Security:** Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, a secure Content Delivery Network (CDN), and Runtime Application Self-Protection (RASP).
- **Data Security:** Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behavior and monitor activity to verify compliance, allowing organizations to prioritize where to allocate their efforts.
- **Identity & Access Management:** Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and Multi-Factor Authentication that help ensure that the right user is granted access to the right resource at the right time.

## Mapping Thales Capabilities to NIS2 Requirements.













Requirement	Article	How Thales helps	Solution Areas
<b>Risk analysis</b>	21.2 (a)	<ul style="list-style-type: none"> <li>Discover and classify potential risk for all public, private and shadow APIs.</li> <li>Identify structured and unstructured sensitive data at risk on-premises and in the cloud.</li> <li>Identify current state of compliance, documenting gaps, and providing a path to full compliance.</li> </ul>	<b>Application Security</b> API Security <b>Data Security</b> Data Discovery & Classification Data Risk Analytics Vulnerability Management
<b>Incident handling</b>	21.2 (b)	<ul style="list-style-type: none"> <li>Speed up incident handling by automatically opening and updating ServiceNow tickets.</li> </ul>	<b>Data Security</b> Ticketing System Integration Workflow Orchestrations
<b>Business continuity, crisis management</b>	21.2 (c)	<ul style="list-style-type: none"> <li>Mitigate of DDoS attacks in as little as three seconds.</li> <li>Implement preventive measures to predict and avoid crisis situations.</li> </ul>	<b>Application Security</b> DDoS Protection <b>Data Security</b> Professional Services Artificial Intelligence
<b>Supply Chain security</b>	21.2 (d)	<ul style="list-style-type: none"> <li>Reduce third-party risk by maintaining on-premises control over encryption keys protecting data hosted in the cloud.</li> <li>Ensure complete separation of roles between cloud provider admins and your organization, restrict access to sensitive data.</li> <li>Monitor anomalies and generate alerts to detect and prevent unwanted activities from disrupting supply chain activities.</li> <li>Enable relationship management with suppliers, partners or any third-party user, with clear delegation of access rights.</li> <li>Minimize privileges by using relationship-based fine-grained authorization.</li> </ul>	<b>Data Security</b> Cloud Key Management Transparent Encryption Data Activity Monitoring User Rights Management Discovery and Classification <b>Identity &amp; Access Management</b> Third-party Access Control Delegated User Management Externalized Authorization
<b>Security in network and information systems</b>	21.2 (e)	<ul style="list-style-type: none"> <li>Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind.</li> <li>Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic.</li> <li>Data activity monitoring for structured and unstructured data across cloud and on-prem systems.</li> </ul>	<b>Application Security</b> Web Application Firewall DDoS Protection Bot Protection <b>Data Security</b> Monitoring Agents and Agentless Data Risk Analytics
<b>Policies and procedures to assess cybersecurity risk-management measures</b>	21.2 (f)	<ul style="list-style-type: none"> <li>Gain full sensitive data activity visibility, track who has access, audit and document what they are doing.</li> </ul>	<b>Data Security</b> Data Governance Reports and Portals

Requirement	Article	How Thales helps	Solution Areas
<b>Use of cryptography and encryption</b>	21.2 (h)	<ul style="list-style-type: none"> <li>• Encrypt data-at-rest on premises, across clouds, and in big data or container environments.</li> <li>• Pseudonymize sensitive information in databases.</li> <li>• Streamline key management in cloud and on-premises environments.</li> <li>• Protect cryptographic keys in a FIPS 140-2 Level 3 environment.</li> <li>• Protect data in motion with high-speed encryption.</li> </ul>	<b>Data Security</b> Transparent Encryption Tokenization Key Management Hardware Security Modules High Speed Encryption
<b>Access control</b>	21.2 (i)	<ul style="list-style-type: none"> <li>• Limit the access of internal and external users to systems and data based on roles and context with policies.</li> <li>• Apply contextual security measures based on risk scoring.</li> <li>• Prevent password fatigue with Smart Single Sign-On with conditional access.</li> <li>• Create frictionless, secure and privacy protected access for your customers.</li> </ul>	<b>Identity &amp; Access Management</b> Workforce Access Management Customer Identity & Access Management (CIAM) Adaptive Access <b>Data Security</b> Transparent Encryption Data Access Blocking Behavioral Analytics
<b>Multi-factor authentication</b>	21.2 (j)	<ul style="list-style-type: none"> <li>• Enable Multi-factor Authentication (MFA) with the broadest range of hardware and software methods and form factors.</li> <li>• Build and deploy adaptive authentication policies based on the sensitivity of the data/application.</li> </ul>	<b>Identity &amp; Access Management</b> Multi-Factor Authentication Risk-based Authentication Hardware and Software Authenticators
<b>Incident reporting</b>	23	<ul style="list-style-type: none"> <li>• A year's worth of retained records are instantly accessible for detailed search and investigation. Audit data is archived automatically but remains accessible in seconds for queries and reporting.</li> </ul>	<b>Data Security</b> Reports and Portals

# Visibility and Control: Thales and Imperva

Thales and Imperva, a Thales company, deliver a broad portfolio of complementary application security, data security, and identity & access management products to provide comprehensive solutions that help address NIS2 requirements. The portfolio delivers comprehensive data-centric security that protects data and all paths to it with platforms that reduce the complexity and risks of managing applications, data, and identities in the cloud.



Applications	Data	Identities
 Web Application Firewall	 Encryption	 Data Activity Monitoring
 DDoS Protection	 Tokenization	 Data Discovery & Classification
 Bot Protection	 Key & Secrets Management	 Data Governance
 API Security	 Hardware Security Modules	 Threat Detection

## Application Security Solutions

### Web Application Firewall (WAF)

Modern web applications are mission-critical for most organizations in all business sectors, and protecting these apps is key for business continuity and resilience. The **Imperva Web Application Firewall** provides out-of-the-box security for web applications, detecting and preventing cyber threats, ensuring seamless operations and peace of mind. Our WAF solution protects against Open Worldwide Application Security Project (OWASP) Top 10 security threats, such as cross-site scripting, illegal resource access, and remote file inclusion, blocking attacks in real time. Our threat research team updates rules that are automatically pushed out daily to ensure our solution protects customers from the latest threats.

### Distributed Denial of Service (DDoS) Protection

DDoS attacks are cybercrimes that attempt to force a website, computer, or online service offline. **Imperva DDoS Protection** provides comprehensive DDoS protection for websites, networks, DNS servers and individual IPs. Our solutions have mitigated the largest attacks in history, immediately and without incurring latency or interfering with legitimate users. Our high-capacity global network holds more than six Terabits per second (6 Tbps) of scrubbing capacity and can process more than 65 billion attack packets per second. This global network of 44+ points of presence (PoPs), each outfitted with a DDoS scrubbing center powered by proprietary Behemoth custom technology, cloud-based WAF, advanced bot mitigation services and more, acts as a software-defined mesh network for optimal performance.

### Bot Protection

The volume of automated threats on the internet is continuously rising, as bad bots account for over thirty percent of all internet traffic. **Imperva Advanced Bot Protection** safeguards mission-critical websites, mobile apps, and APIs from automated threats and online fraud without affecting the flow of business-critical traffic. It defends customers against web scraping, account takeover, scalping, transaction fraud, gift card fraud, denial of service, competitive data mining, unauthorized vulnerability scans, spam, click fraud, and web and mobile API abuse.

### API Security

Whether developing applications in new cloud-native microservice and serverless architectures, automating business-to-business processes, or providing a back-end for mobile applications, APIs are essential to the modern enterprise. Through automatic discovery and continuous monitoring of API endpoints, **Imperva API Security** enables comprehensive API visibility for security teams – without requiring development to publish APIs via OpenAPI or by adding resource-intensive workflow to their CI/CD processes. Moreover, every time an API is updated, security teams can stay on top of the change, understand any new risks, and incorporate changes, which leads to faster, more-secure software release cycles. Imperva API Security enables security teams to keep pace with innovation without impacting development velocity.

# Data Security Solutions

## Data Discovery and Classification

A crucial first step to aligning with the NIS2 framework is understanding what constitutes sensitive data, where and how it is stored, and who can access it. **CipherTrust Data Discovery & Classification** discovers and classifies data in all the data stores in an organization's data estate, from structured to semi-structured to unstructured across on-premises, hybrid, cloud, and multi-cloud environments. This visibility enables organizations to build a strong data privacy and security foundation.

## Data Access Monitoring

Continuous monitoring captures and analyzes all data store activity, in the cloud or on-premises, for both application and privileged user accounts, providing detailed audit trails that show who accessed what data, when, and what was done to the data. **Imperva Data Security Fabric Data Activity Monitoring (DAM)** unifies auditing across diverse on-premises platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. It also supports databases hosted in Microsoft Azure and Amazon Web Services (AWS), including PaaS offerings such as Azure SQL and Amazon Relational Database Services (RDS). Detailed data activity is captured automatically, making it easier to fulfill audit requests.

## Threat Detection

Threat detection is one of the most important capabilities to prevent or identify and respond to a cyberattack. **Imperva Data Security Fabric Threat Detection** monitors data access and activity for all databases and provides the visibility needed to pinpoint risky data access activity for all users, including privileged users. Organizations can uncover hidden risks and vulnerabilities while creating reports to effectively communicate risk and ongoing activities. It delivers real-time alerting and user access blocking of policy violations and cost-effectively retains years of data for audits.

Combining deep domain security expertise with machine learning (ML) allows organizations to identify suspicious user and computer system behaviors that violate security policies, practices, and peer group norms. Purpose-built detection algorithms instantly recognize active attack exploits and immediately send incident alerts.

## Encryption

Encryption plays an important role in protecting data's confidentiality, integrity, and availability across its lifecycle: at rest, in-motion, and in use.

- **Data at Rest**

Depending on your security requirements and infrastructure, different approaches can be used to protect data-at-rest in files, volumes, and databases. **CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Transparent Encryption operates at the file system layer, delivering data-at-rest encryption with centralized key management, granular access controls, and data access logging to meet best practice requirements for protecting data. To protect data-at-rest from zero-day and privileged escalation attacks, ransomware protection uses real-time behavior monitoring to alert or block malicious activity before ransomware can take hold of data. Database protection at the database layer supports key management for native TDE use cases or the ability to do field or column-level encryption on databases. At the application layer, libraries for C and Java can be deployed, or solutions at the network layer can be used as a gateway to apply encryption without modifying the application code.

- **Data in Motion**

Protecting data in-motion is essential to prevent from eavesdropping, surveillance, and overt and covert interception of sensitive data. **Thales High Speed Encryption** provides certified, network-independent, data-in-motion encryption (layers 2, 3, and 4), ensuring data is secure as it moves from site to site or from on-premises to the cloud and back, allowing customers to better protect data, video, voice, and metadata flowing between repositories. The network encryption solution has been proven to deliver maximum uptime in the most demanding, performance-intensive environments. It has near-zero latency and can operate in full-duplex mode at full-line speed while offering flexible and vendor-agnostic interoperability, meaning it's compatible with all the leading network vendors throughout your network.

## Tokenization

Tokenizing or masking data reduces the cost and effort required to comply with internal security policies, industry frameworks, and regulatory mandates, such as NIS2, the European Union's Global Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI-DSS). CipherTrust Tokenization permits the pseudonymization of sensitive information in databases so you can analyze aggregate data without exposing sensitive data during analysis. It offers application-level tokenization services in two convenient solutions that deliver complete customer flexibility: Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization. Both solutions secure and anonymize sensitive assets, whether they reside in the data center, big data environments, or the cloud.



## Key & Secrets Management

Centralized key management consolidates on-prem and cloud encryption keys, so you can apply consistent security policies across multiple file servers, databases, applications, virtual machines, and cloud platforms. **CipherTrust Key Management** provides a greater command over your keys and simplifies key lifecycle management tasks while enhancing data security through consistent enforcement of key policies, fine-grained access control, and robust auditing and reporting of all key management and encryption operations.

Modern development trends such as containerization, cloud transformation, DevOps, and automation have contributed to a massive increase in the use of secrets (credentials, certificates, keys) for authentication, which can be vulnerable to cyber-attacks when not securely managed.

**CipherTrust Secrets Management** protects and automates access to mission-critical secrets across DevOps tools and cloud workloads, including secrets, credentials, certificates, API keys, and tokens, to help security and governance teams reduce risk by streamlining security processes.

## Data Governance

Organizations need to monitor files and databases across hybrid IT to help ensure data is secure, private, accurate, available, and usable.

**Imperva Data Security Fabric** includes discovering and mapping file and database servers and identifying sensitive data such as social security numbers, credit card data, etc. It allows organizations to understand current data usage, enabling role and workflow management of data to grant access to data stewards and creating reports around data to measure effective alignment to NIS2 and other regulation requirements.

## Hardware Security Modules

A hardware security module (HSM) is a dedicated crypto processor that protects the crypto key lifecycle. It acts as a trust anchor that protects the cryptographic infrastructure of some of the world's most security-conscious organizations by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. **Thales Luna Hardware Security Modules** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. They are available on-premises, in the cloud as-a-service, and across hybrid environments.

Luna HSMs generate and protect root and certificate authority (CA) keys, supporting PKIs across various use cases. They sign the application code to ensure the software remains secure, unaltered, and authentic. They create digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other deployments.

# Identity & Access Management Solutions

## Customer Identity & Access Management

Customer Identity & Access Management (CIAM) manages access for identities external to an organization such as the identities of customers, gig workers, suppliers, or partners. **Thales OneWelcome Identity Platform** provides a consistent identity experience across all customer touchpoints, allowing organizations to balance security and usability to enable a frictionless experience at scale for customers— regardless of their location, device, or application. The Platform enables organizations to thrive in a regulated market, helping them meet requirements of local, national and international data regulations with a CIAM solution that can handle the most complex data privacy and protection regulations.

## Workforce Identity & Access Management

A disproportionate number of data breaches start with unauthorized access of data and sensitive resources, credential compromise, and privilege abuse. **Thales SafeNet Trusted Access** is a cloud-based access management solution that makes it easy to manage access both to cloud services and to enterprise applications with an integrated platform combining single sign-on (SSO), multi-factor authentication (MFA), and scenario-based access policies. SafeNet Trusted Access provides a single pane view of access events across an organization's app estate to ensure that the right user has access to the right application at the right level of trust. SafeNet Trusted Access allows organizations to virtually (or logically) limit the access to confidential resources through use of MFA (including phishing-resistant authentication) and granular access policies.

## Broadest Range of Authentication Solutions

Multi-factor authentication is a requirement of NIS2 and most other regulations and standards. **Thales OneWelcome Authenticators** include a broad range of hardware and software authentication methods and form factors for workforce and external users. These include phishing-resistant authentication capabilities, such as CBA and FIDO, in addition to a user-friendly smartphone-based authenticator app called MobilePASS+. External users, including customers or partners, also have nuanced authentication needs. With the OneWelcome Identity Platform, organizations can enable both low-assurance and high-assurance authentication mechanisms, including SCA (Strong Customer Authentication) or use of FIDO Passkeys.

## Conclusion

The NIS2 directive dramatically raises the bar for cyber risk management and incident reporting obligations across the EU for the majority of public or private organizations. Its strict reporting requirements ensure no covered organization can ignore it without risking major penalties. Even organizations not considered “essential”, such as manufacturers and online portals can be subject to targeted audits, on-site inspections, requests for information, and random checks.

Drawing on decades of experience helping corporate entities and public enterprises adhere to compliance mandates, Thales offers a broad range of products and services that enable organizations to strengthen cyber resilience, address the security of supply chains, streamline reporting obligations, and comply with the more stringent supervisory measures and stricter enforcement requirements of NIS2.

Moreover, the combined Thales and Imperva portfolios help simplify compliance across multiple overlapping regulatory regimes in addition to NIS2, such as GDPR and DORA, or standards such as ISO 27001, PCI, or the NIST Cybersecurity Framework 2.0. Our portfolio delivers unparalleled centralized visibility and control over data, application, and access control security, helping automate security and compliance processes and reducing the burden on security and compliance teams.

## About Thales

As the global leader in data security, Thales helps the most trusted brands and organizations around the world protect their most sensitive data and software, secure the cloud, provide seamless digital experiences, and achieve compliance through our industry-leading application security, data security & governance, identity and access management, and software licensing solutions. Thales completed its acquisition of Imperva on December 4, 2023.

# THALES

Building a future we can all trust

## Contact us

For all office locations and contact information,  
please visit [cpl.thalesgroup.com/contact-us](https://cpl.thalesgroup.com/contact-us)

[cpl.thalesgroup.com](https://cpl.thalesgroup.com)

