yubico

NIS2 DIRECTIVE

Prepare for NIS2 Compliance with the YubiKey

16 January 2023
NIS2 entered into force

17 October 2024
Member state deadline to transform directive into national **law**

18 October 2024
Member state deadline to **apply** new measures

15 sectors covered

Penalty for **essential** entities

Up to €10M

or 2% annual revenue whichever is higher

Penalty for **important** entities

Up to €7M

or 1.4% annual revenue whichever is higher

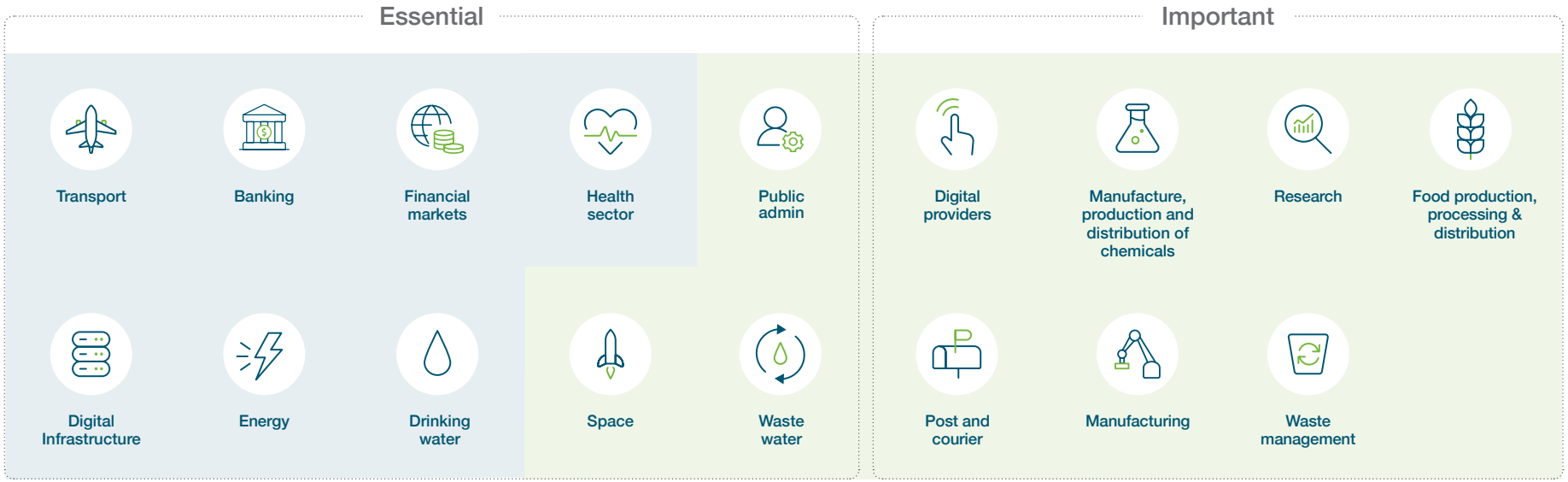
What is the NIS2 Directive?

The Network and Information Security (NIS) Directive was introduced in 2016 as a legal framework for cybersecurity standards across the EU. The NIS2 Directive is an update and scope expansion which entered into force in January 2023.[1]

NIS2 introduces new security requirements and supervisory measures, and covers more entities from a wider range of sectors, and their supply chain partners. Member states have until 17 October 2024 to transpose NIS2 Directive measures into their own respective national laws. Enforcement of new security measures begins on 18 October 2024, creating immediate regulatory requirements for enterprises operating or carrying out activities within the EU.[2]

Who needs to comply with NIS2?

NIS2 impacts all organisations, companies and suppliers providing essential or important services, a distinction which impacts the level of oversight and potential fines for non-compliance. NIS2 expands upon the scope of the NIS Directive to oblige even more organisations to reinforce their cybersecurity practices based on their importance to society.



Until member states create lists of who must comply, organisations should assume NIS2 will apply to them, if the following criteria is met:

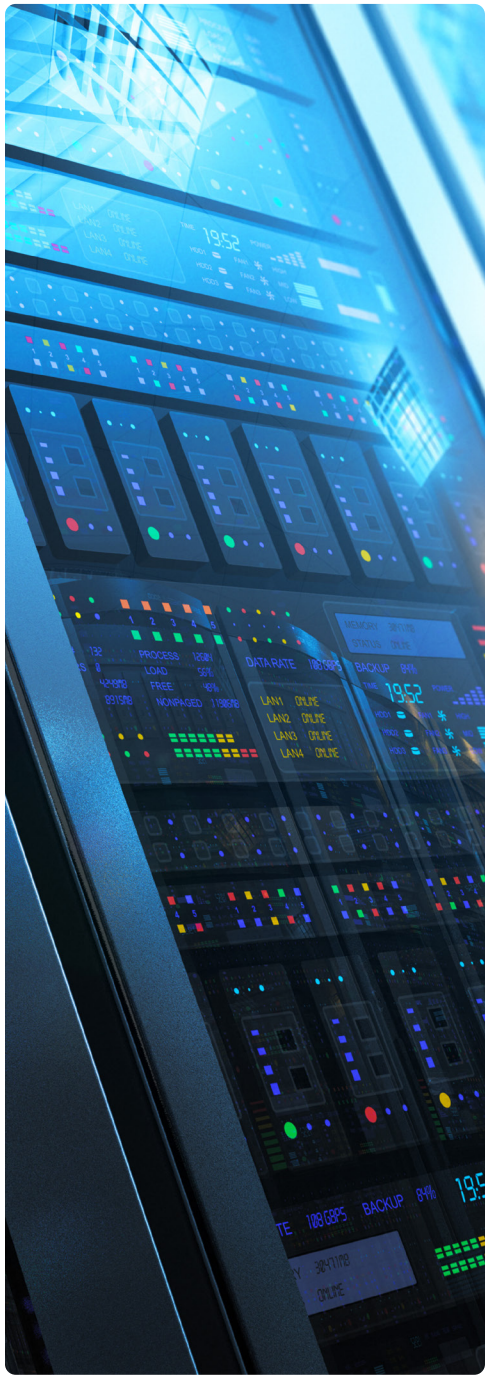
One of the 15 essential or important sectors

+

ESSENTIAL	IMPORTANT
Large organisation 250+ employees or €50M+ in turnover	Medium organisation 50+ employees or €10M+ in turnover

or

High risk or sole provider of a service
any size



NIS2 introduces stricter requirements

The first NIS Directive required operators of essential services and digital service providers to adopt technical and organisational measures appropriate and proportionate to risk, taking into account the security of systems and facilities, incident handling, business continuity management, monitoring, auditing and testing, and compliance with international standards. This broad remit resulted in significant gaps in how member states laid out their requirements.

To strengthen overall cybersecurity throughout the EU, NIS2 now requires minimum technical, operational and organisational obligations across both organisations and their supply chains:

10 elements for all covered entities

Policies and procedures to assess security measures	Cyber hygiene practices (e.g., Zero Trust) and cybersecurity training	Cryptography and encryption policies	Access control policies	The use of multi-factor authentication (MFA)*
Risk analysis and information security policies	Supply chain security	Incident handling	Business continuity planning	Network and information system security

NIS Directive | **Added in NIS2**

* or continuous authentication and, where appropriate, secured communications

NIS2 also includes a framework for incident reporting requirements and for supervisory and enforcement activities (e.g., audits) by member states, differentiated across essential and important entities. Furthermore, to strengthen compliance with security measures, NIS2 mandates penalties of up to €7M for important entities or €10M for essential entities, or 1.4% or 2% of annual revenue, respectively. As such, it is essential for all covered entities to implement measures to reduce the risk of compromising incidents, including adopting strong access and identity management controls.

Not all MFA is created equal

When deploying MFA to comply with NIS2, organisations should select an authenticator based on its strength, referencing the global NIST standard[3] or eIDAS[4]. These guidelines recognize that **not all MFA is created equal**, represented through Authentication Assurance Levels/Levels of Assurance (AALs/LoAs). While any form of MFA is better than a password alone (AAL1/LoA Low), legacy forms of MFA (AAL2/LoA substantial) such as SMS, mobile authentication and one-time passcodes (OTP) experience a 10-24% attack penetration rate[5] while a phishing-resistant hardware-based authenticator (AAL3/LoA high) offers higher assurance, meeting NIS2 requirements and reducing the threat of account compromise.[6]

AAL1	AAL2	AAL3
Single-factor authentication e.g., username and password	**Two-step authentication** e.g., 2FA, synced passkeys, device-bound passkeys on general purpose devices	**Hardware-based multi-factor authentication** e.g., device-bound passkeys on hardware security keys
• Low security assurance • Highly vulnerable to phishing • Puts enterprises at risk	• Phishing-resistant 2FA/MFA • Stronger security than a password but vulnerable to attacks • More enterprise-ready but leaves gaps in operational efficiency and audit/compliance requirements	• Phishing-resistant MFA • Strongest security and highest assurance • Addresses enterprise security, operational efficiency and audit/compliance requirements • Supports FIDO and Smart Card/PIV • FIPS 140-2 validated

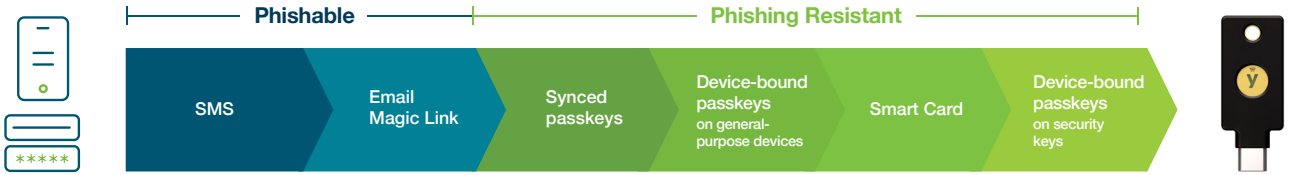
Learn more in our Zero Trust white paper
yubi.co/zerotrust-wp

Zero Trust as a cyber hygiene practice

While NIS2 does not explicitly specify the exact technological measures to enact, Zero Trust is referenced as a cyber hygiene practice for all essential and important entities. A Zero Trust strategy, predicated upon the concept of “never trust, always verify”, shifts security controls from the traditional network perimeter toward an identity-based approach, by implementing strong authentication and granular access control policies as well as encryption and key management.

The Zero Trust Maturity Model (ZTMM),[7] developed by the US Cybersecurity and Infrastructure Security Agency (CISA), offers a framework for the journey from a traditional starting point to Initial, Advance and Optimal Zero Trust. At each stage, the ZTMM requires stronger forms of MFA be adopted, progressing toward the exclusive use of **phishing-resistant MFA**, which relies on cryptographic verification between devices or between a device and a domain, making the authentication process immune to attempted compromise or subversion.

Fast-track NIS2 compliance with the YubiKey



The YubiKey family
The YubiKey is availablein multiple form factors for desktops, laptops and mobile devices.

The YubiKey is a hardware security key built to create organisations of phishing-resistant users. As a hardware root of trust, the YubiKey offers highest-assurance phishing-resistant authentication. Manufactured and programmed in Sweden by Yubico, a Swedish company, the YubiKey is certified against FIPS and FIDO.

Supporting both Smart Card/PIV and FIDO2 (Passkey) protocols, as well as FIDO U2F, OTP/TOTP and OpenPGP, the YubiKey meets you where you are on your cybersecurity journey, and suits a wide range of business scenarios.

- Privileged access
- Mobile restricted
- Shared workstations
- Remote workforce
- Office workers
- 3rd-party access
- End customers

Ensure compliance with NIS2 MFA requirements by implementing the YubiKey today. For high assurance across your supply chain, require that all suppliers implement phishing-resistant MFA for their own users and systems.

The total economic impact of YubiKeys[7]:

Strongest security

Reduce risk by

99.9%

High return

Experience ROI of

203%

Faster

Decrease time to authenticate by

>4x

Durable

IP68 rated, crush resistant, no battery required, no moving parts

The YubiHSM 2 and the YubiHSM 2 FIPS

Game changing cryptographic protection for servers, applications and computing devices.

How the YubiKey helps address authentication challenges for critical infrastructure

Many NIS2 essential or important entities rely on legacy production equipment, shared workstations and mobile-restricted environments. The YubiKey is an ideal option for complex critical infrastructure organisations, providing the flexibility to navigate between devices and across hundreds of products, services and applications, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with secrets never shared between services. The YubiKey doesn't require additional hardware, software, external power, batteries or network connection. Secure authentication is simple: plug the YubiKey into a USB port and touch the button, or tap for NFC.

Satisfy NIS2 encryption and cryptography requirements with YubiHSM 2

The YubiHSM 2 is purpose-built to enable compliance, store and generate cryptographic keys, safeguard secrets and perform cryptographic operations, satisfying NIS2 encryption requirements for your organisation, supply chain partners, and so protecting your entire Software Bill of Materials (SBOM). The world's smallest Hardware Security Module (HSM), with support for common interfaces such as PKCS11 and Microsoft CNG, the YubiHSM 2 is ideal for:

PKI

Secure your Public Key Infrastructure with confidence by entrusting the generation and safeguarding of your Root CA and Issuing CA private keys to the YubiHSM 2.

Code signing

Protect the integrity of your applications against third-party interference by generating and storing your code signing private key on the YubiHSM 2.

Database encryption

Safeguard information from unauthorized access by encrypting sensitive information and securely storing encryption keys within the YubHSM 2.

IoT

Improve your IoT device and autonomous solutions security with the compact power of the YubiHSM 2, ensuring integrity and the confidentiality of your operations.

Defence

Ensure the integrity of data and communications exchanged between land, aerial and sea assets with the resilient security of the field-removable YubiHSM 2.

Contact us
yubi.co/contact

Learn more
yubi.co/yk5

Sources

[1] Official Journal of the European Union, Directive (EU) 2016/1148, (December 14, 2022)

[2] European Parliament, The NIS2 Directive, (February 2023)

[3] NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022)

[4] European Commission, eIDAS Levels of Assurance (LoA), (2014)

[5] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[6] Office of the European Union, Commission Implementing Regulation (EU) 2015/1502, (September 2015)

[7] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

yubico

About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

For more information, please visit: www.yubico.com.