COLORTOKENS

A Guide To
NIS Directive and NIS 2.0 Proposal

WHITE PAPER

Table of Contents

Overview

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation, which entered into force in 2016, to achieve a high common level of cybersecurity across the Member States. Businesses identified as operators of essential services, or providers of digital services will have to comply with the security requirements under the directive (Arts. 5, 6 NIS Directive). For example, Member States have to designate competent authorities for monitoring compliance with the Directive and set up computer security incident response teams (CSIRTs).

NIS Directive has helped in implementing stronger and stricter security safeguards, and has led to a general improvement in cyber defense capability among critical infrastructure-like entities. However, it is no longer sufficient to tackle the growing threats posed with digitalisation and the surge in cyber-attacks, as it does not cover all digitised sectors that offer essential services to the community. In order to strengthen the security requirements needed to address supply chain attacks, streamline reporting obligations, and introduce more stringent supervisory measures and enforcement requirements, including harmonised sanctions across the EU, the Commission submitted a proposal in 2020 to reform the NIS Directive and introduced the NIS 2.0 draft.

The NIS 2.0 proposal builds on and repeals the NIS Directive. In addition to the sectors already covered by the NIS Directive, the draft NIS 2.0 has proposed to include other essential facilities in the sewage, public administration and space sectors. The differentiation between operators of essential services and providers of digital services has been abandoned. Instead, services are now categorised as “essential” and “important” based on the degree of criticality of the sector (rec. 11 of the draft NIS2 Directive). This expansion of the scope covered by the draft NIS 2.0 would boost the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

This whitepaper provides an analysis of the existing NIS Directive and the draft NIS 2.0, and helps the reader recognise how ColorTokens Xtended ZeroTrust™ Platform addresses the stringent requirements dictated by the Draft 2.0 Directive and enables organisations across Europe to become cybersecurity ready for the digital age. ColorTokens’ range of products and services are well suited to meet the core objectives of the Directive - protection against advanced cyberattacks, discovery and detection of cybersecurity events. In addition to this, ColorTokens Zero Trust Access Solution, Xaccess, facilitates secure digitization by ensuring least privilege access for local or remote users to the critical application or workload segment irrespective of the location of the user or the application, making it one of the best solutions in the market for secure remote access which is the need of the hour.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[2] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

Introduction to NIS Directive

Background

The first EU Directive on Security of Network and Information Systems (NIS Directive) was introduced in 2016. The law required participating states that provide critical infrastructure and digital services to have appropriate security measures to manage cyber risk and maintain resilience. To raise the cybersecurity preparedness level of the Critical National Infrastructures (CNI) across EU Member States, the original NIS Directive defined following objectives that are still considered as very relevant:

- Increase the capabilities of Member States in mitigating cybersecurity risks and handling incidents.
- Improve the level of cooperation amongst Member States in cybersecurity and the protection of essential services.
- Promote a culture of cybersecurity across all sectors vital for Europe's economy and society that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

It applies to industries providing essential services to society such as Energy, Water, Transport, Health and Finance. The interpretation of which companies fall within scope across these industries is a matter for individual Member States. NIS Directive was transposed into UK law in 2018 as the NIS Regulations. These regulations are still in place following the UK's departure from the European Union and will be reviewed by the UK Government during 2021.

Objectives

The UK National Cyber Security Centre (NCSC) produced a collection of guidance for the implementation of the UK NIS Regulations. Figure 1 outlines the principles and objectives that are defined in the NIS Guidance Collection . The original NIS principles are further outlined in Table 1; this provides an overview of what is expected of each operator of essential services as defined under the NIS Regulations.

[3] https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance

NIS Objectives

Objective A
managing security risk

Objective B
Protecting against cyber attack

Objective C
Detecting cyber security events enter

Objective D
Minimizing the impact of cyber security incidents

NIS Principles

A1
Governance

A2
Risk Management

A3
Common Asset Management

A4
Colin Supply Chain

B1
Service Protection Policies and Processes

B2
Identity and access control

B3
Data Security

B4
System Security

B5
Resilient Netwerk and Systems

B6
Stuff Awareness and Training Governance

C1
Security Monitoring

C2
Proactive Security event Discovery

D1
Response and Recovery Planning

D2
Lessons Learned

Objective A
Appropriate organizational structures, policies, and processes in place to understand, assess and systematically manage security risks to essential services.

Objective B
Proportionate security measures in place to protect essential services and systems from cyber-attack. includes: identity and access control, data and service security, informational protection policies and processes, protective technology and stuff awareness and training.

Objective C
Capabilities to ensure security defenses remain effective and to detect cyber security events affecting, or with potential to affect, essential services. Includes security monitoring and anomaly detection.

Objective D
Capabilities to minimize the impacts of cybersecurity incident on the delivery of essential services including the restoration of those services were necessary. Includes response and recovery plans.

Regulated Sectors

The NIS Regulations are applicable on operators of essential as well as digital services and require them to comply with security precautions and reporting obligations. An essential service must, according to the criteria of the NIS Directive (Arts. 5, 6 NIS Directive), be indispensable for the maintenance of critical social and economic activities, and be dependent on a network and information system. The providers of digital services, must include online marketplaces, cloud computing services and search engines, and are subject to similar obligations The sectors of essential and digital services covered by the NIS Directive are listed below:

Table 2: List of Regulated Sectors by NIS Directive

Operators of Essential Services	Providers of Digital Services
Healthcare Providers	Cloud Services
Digital Infrastructure – IXPs, DNS Services	Online Marketplaces
Transport	Online Search Services
Drinking Water	
Financial Market Infrastructure	
Energy	
Banking	

[4] http://eprints.gla.ac.uk/240966/1/240966.pdf

[5] https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance

Reform of the NIS Directive: Draft NIS 2.0

The threat landscape has changed considerably since the NIS Directive came into force in 2016, and the scope of the directive needs updating and expanding to meet current risks and future challenges, one such challenge being to ensure that 5G technology is secure. Since the onset of the coronavirus crisis, the EU economy has grown more dependent on network and information systems than ever before, and sectors and services are increasingly interconnected. The pandemic has more than confirmed the importance of preparing the EU for the digital decade as well as the need to continually improve cyber-resilience, particularly for those who operate essential services such as healthcare and energy. Clearly, NIS Directive is no longer sufficient to ensure absolute cyber defence against the ever evolving cyber threats.

The Commission also criticised the implementation of the NIS Directive by the Member States, including often poorly enforced sanctions, insufficient exchanges at Union level in certain areas and, in particular, a lack of harmonisation between Member States regarding the categorisation of cyber security incidents. Shortcomings of the old Directive were also pointed out, such as the high regulatory burden for the competent authorities of the Member States and the overly narrow scope of application, which does not cover all digitalised sectors that offer essential services to the community. In line with the criticism expressed by the Commission on the state of implementation of the NIS Directive, the initiative was therefore taken to revise the NIS Directive and extend the scope of its application to further sectors.

Broader scope of application

The proposed draft NIS 2.0 has renamed the categories defined by the old NIS Directive, expanded the number of regulated sectors, and significantly expanded the types of entities that fall within these sectors. In addition to the sectors already covered by the old Directive, essential facilities in the sewage, public administration and space sectors are now also included in NIS 2.0. The earlier categories of "essential services" and "digital services" have been abandoned, and new categories of "essential" and "important" facilities are introduced on the basis of the degree of the criticality of the sector.

Under NIS 1, Member States created a list of regulated organisations on the basis of how strategically important the entities are to the State (i.e., market size, national security, economic impact, etc.). However, under NIS 2, the Member States do not designate a specific organization as regulated. Instead, NIS 2 would require all essential and important entities to register with ENISA, and ENISA would notify Member States of entities in their jurisdiction.

[6] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

Below is the revised and expanded list of sectors covered by NIS 2.0:

Table 3: List of Regulated Sectors by draft NIS 2.0

Essential Entities	Important Entities
All sectors covered by NIS Directive	Social Networking Services
Additional health-related services – including pharma, some medical device manufacturers, researchers.	Online Marketplaces
Additional digital infrastructure services – cloud computing services, data centers, CDNs, network providers	Online Search Services
Waste Water	Food Production and Distribution
Space	Postal Services
Public Administration	Waste Management
	Chemical Manufacturers
	Manufacturing – medical devices, electronic devices, machinery, vehicles and transport equipment

Revised Security Requirements & Penalties

The security requirements and measures prescribed by the draft NIS 2.0 for operators of essential and important services are now described more comprehensively and uniformly. The NIS 2 Directive would empower Member States to require essential and important entities to certify ICT products, services, and processes under specific EU cybersecurity certification schemes. [NIS 2, Art. 21] The proposed NIS 2 Directive would also expand on the security outcomes required under NIS 1, with a notable new section on supply chain security and a burdensome expansion of requirements to report any potential cyber threat that could cause a disruption.

Here is a brief summary of the revised security measures under NIS 2.0 Proposal:

Objectives	NIS 2.0 Proposal
Security Program	Essential and Important entities must take appropriate technical and organizational measures to manage risks to the security of networks and information systems. [NIS 2, Art. 18.1]
Risk Assessment	Measures taken for the security of networks and information systems must be appropriate to the risks and reflect the state of the art. Periodic Risk Analysis should also be performed. [NIS 2, Art.18.2(a)]
Security Safeguards	**Security measures for essential and important services shall include at minimum:** • Incident prevention, detection, and response. • Business continuity and crisis management. • Secure network and systems acquisition and maintenance, including vulnerability handling and disclosure. • Testing and auditing safeguard effectiveness. • Use of cryptography. [NIS 2, Art. 18.2]

Objectives	NIS 2.0 Proposal
Supply chain	Essential and important services must include supply chain in their security measures [NIS 2, Art. 18.2(d)]. They must consider specific suppliers' vulnerabilities and cybersecurity practices [NIS 2, Art. 18.3]. Supply chain includes network and systems acquisitions, data storage and processing services, and managed security services. [NIS 2, Art. 18.2(d)-(e)].
Workforce and Personnel	The management of essential and important entities must approve their respective cybersecurity risk management measures, and follow regular cybersecurity training. [NIS 2, Art. 17]
Incident reporting	Notify the relevant competent authority and, where applicable, their customers of "any significant cyber threat" that "could have potentially resulted" in a substantial disruption or loss. [NIS 2, Art. 20.1-3]

In future, the national authorities will be taking on more responsibilities for monitoring and enforcing the regulations. The NIS 2 Directive contains a catalogue of measures and powers that the Member States must follow(Art. 29 et seq. draft NIS 2 Directive). The framework for penalties throughout Europe provides for fines of at least up to 10 million Euros / 2% of the worldwide annual turnover.

The proposal thus offers a reformed version of the previous regulation within the framework of NIS 1.0 and shows that the NIS Directive is not sufficient to respond to the growing threats posed by digitalisation, and proves that the aim is to tighten the legal obligations and achieve greater EU-wide harmonisation.

Next Steps for NIS 2

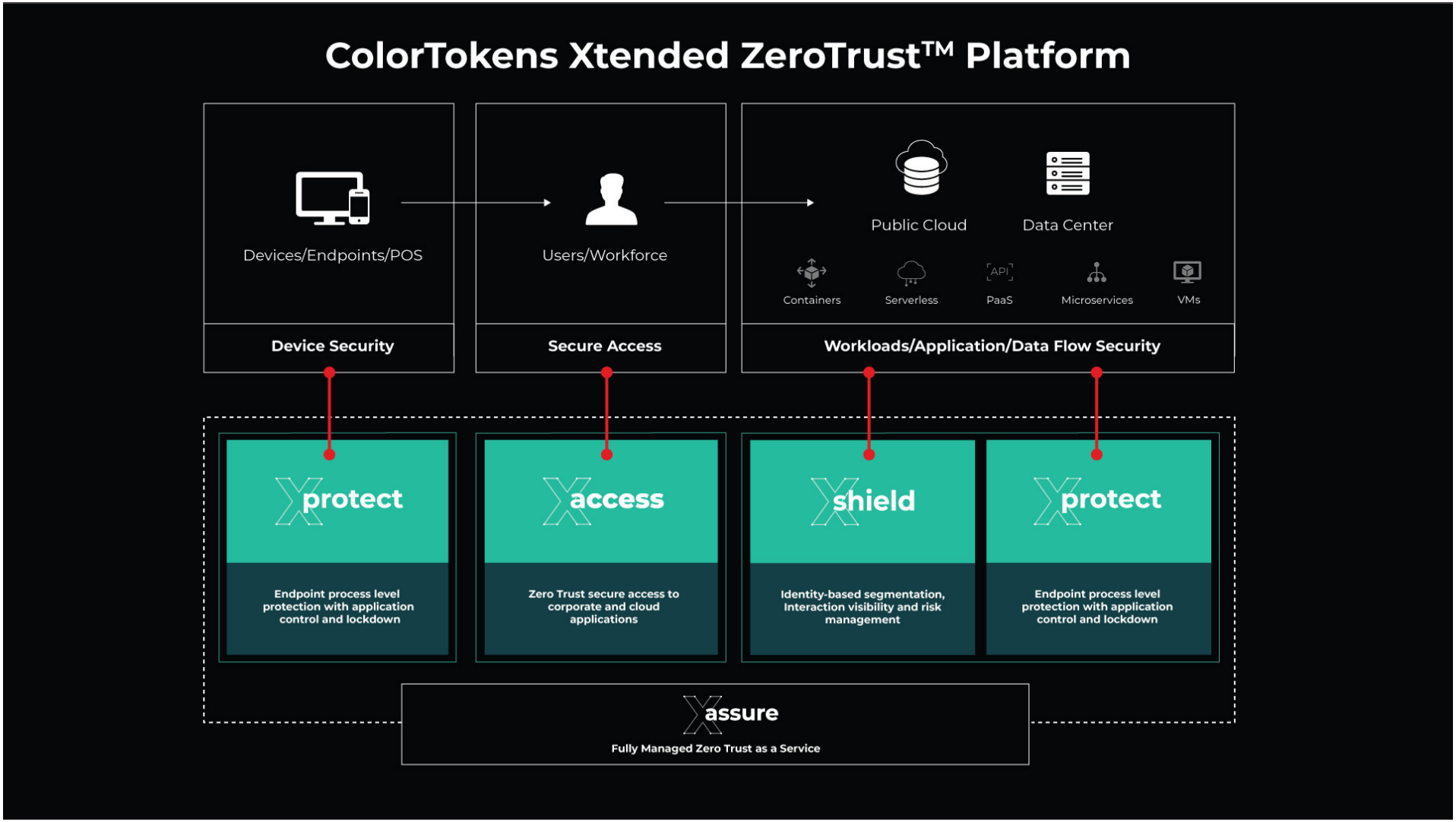
The proposed draft NIS 2 is now subject to negotiations between the EU Council and the EU Parliament, and they have to take a position on the proposal. There is no official public deadline for these negotiations, but it's likely to happen in next few months. After entry into force, the Member States are to transpose the Directive into national law within 18 months [NIS 2, Art. 38].

How ColorTokens can help

ColorTokens Xtended ZeroTrust™ Platform supports organizations in meeting the Objectives B and C (refer Table 1). Objective B can be served well using the ColorTokens suite of cybersecurity products whereas Objective C could be met by ColorTokens' managed services, Xassure, that offer Zero Trust as a service.

Objective	Principles	How the ColorTokens Xtended ZeroTrust™ Platform Addresses the Requirement
Objective B – Protection against Cyber Attack	B1. Service Protection Policies and Processes Defining and communicating appropriate organizational policies that help secure systems and support operation of essential functions.	In-depth visibility and control for managed workloads with Xshield and Xprotect. Visibility provided into network traffic and processes ensures that critical functions are adhering to the defined organizational policies. For example, a critical infrastructure application should not be communicating with another HR application. A critical application should not be running an SMB process. ColorTokens products alert on anomalies, enforce strict controls, and leverage micro-segmentation to ensure a Zero Trust environment for applications where every communication is validated and access governed by the principle of least privilege. They ensure granular controls and help in enforcement of defined organizational policies.

Objective	Principles	How the ColorTokens Xtended ZeroTrust™ Platform Addresses the Requirement
	B2. Identity and Access Control Understanding, documenting and controlling access to networks and information systems supporting essential functions	ColorTokens ZTNA solution, Xaccess, provides identity- based granular access control to applications/systems running in the Datacenter. User Identity from multiple Identity Providers (IdPs) can be used to grant, deny or provide restricted access irrespective of whether the user is on premises or remotely located. Control can be based on several user attributes available in the identity store such as Department, Groups etc. For example, an Administrator will be granted access to a Linux server on port 22 upon validating his/her credentials and group membership but all other users may only be granted access on port 443. Similarly, Finance applications can only be accessed by users belonging to Finance department.
	B3. Data security Protecting stored or electronically transmitted data from actions that may cause an adverse impact on essential functions	ColorTokens can help encrypt data in transit by creating tunnels between the managed workloads. Application 1 can talk to Application 2 via an encrypted tunnel to prevent traffic snooping. Securing data at rest or within the application is beyond the scope of ColorTokens platform.
	B4. System Security Protecting critical network and information systems and technology from cyberattack.	ColorTokens aims at providing an integrated Zero Trust platform for hybrid networks that combines the power of Zero Trust Network Access, Micro-segmentation, Process Control, and server workload protection. Increasingly, companies and even nations are adopting the Zero Trust model to protect critical infrastructure applications. ColorTokens suite of products simplifies Zero Trust adoption for enterprises and helps to: A) Reduce the attack surface and prevent lateral movement B) Decrease risks of remote access C) Minimize the impact of breaches ColorTokens Xtended ZeroTrust™ Platform provides protection across multiple touch points as highlighted below:


ColorTokens Xtended ZeroTrust™ Platform
Devices/Endpoints/POS
Users/Workforce
Public Cloud
Data Center
Containers
Serverless
PaaS
Microservices
VMs
Device Security
Secure Access
Workloads/Application/Data Flow Security
xprotect
Endpoint process level protection with application control and lockdown
xaccess
Zero Trust secure access to corporate and cloud applications
xshield
Identity-based segmentation, Interaction visibility and risk management
xprotect
Endpoint process level protection with application control and lockdown
xassure
Fully Managed Zero Trust as a Service

Objective	Principles	How the ColorTokens Xtended ZeroTrust™ Platform Addresses the Requirement
	B5. Resilient networks and systems Building resilience against cyber attacks	After successfully exploiting a weakness, the attacker typically moves laterally to find critical targets. Micro-segmentation provided by Xshield is a layer that blocks lateral movement and adds resilience. Xprotect's server workload protection adds another layer. ColorTokens' layered security approach helps in delaying these attacks, thereby providing SOC teams with enough time to adapt or detect and respond. ColorTokens can also automatically quarantine systems, that are known to be compromised, for immediate and automated response.
Objective C – Detecting cyber security events	C1. Security Monitoring Monitoring to detect potential security problems and track the effectiveness of security measures	ColorTokens offers 24/7 managed security service, Xassure, that delivers Zero Trust as a service and tracks down the most elusive threats with just-in-time detection and response. Xassure's Advanced Threat Monitoring (ATM) is an Extended Detection and Response (XDR) service providing holistic detection capabilities. Xassure ATM correlates endpoint and network telemetry to hunt for threats. The service provides higher confidence and actionable alerts, resulting in lower alert fatigue. The service also offers blast radius analysis, thereby tracking the effectiveness of applied security measures. The ATM service offers the following: • Deep monitoring using patterns, signature and reputation check • Custom threat alerts • Threat intel for bad hash, IP and domain • APT detection • Review of operations effectiveness
	C2. Proactive Security Event Discovery Detecting anomalous events in relevant network and information systems	• Xassure provides Breach Protection Service (BPS). Leveraging the telemetry from endpoints and network, it protects against advanced cyberattacks such as hidden attacks, APTs and data breaches using a combination of AI/ML and certified Threat Hunters.

NIS Toolkit

NIS Directive (EU) of the European Parliament and the Council of the European Union
NIS2 Directive: A high common level of cybersecurity in the EU.
NIS 2.0 Draft
Interorganisational Cooperation in Supply Chain Cybersecurity

For more information on how ColorTokens can help your organization comply with security requirements, please visit https://colortokens.com/products/xtended-zero-trust-platform/ .

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically.

As cloud adoption grows, traditional perimeters get redefined, and new attack vectors and threat actors materialize, corporations recognize their security posture needs to reflect their Zero Trust philosophy. ColorTokens' technology allows customers to achieve Zero Trust by utilizing rich, meaningful contextual information about the application, microservice, or protected resource, so customers can apply Zero Trust with as secure of a perimeter as they can. ColorTokens' cloud-based SaaS platform can automatically deploy next-generation security controls and increase security posture dynamically without any new hardware, downtime, reboots, or changes to a client's existing systems.

With a team of over 400 people, ColorTokens has global office locations in Santa Clara, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit **www.colortokens.com.**