BELDEN

WHITE PAPER

Your Guide to the Network and Information Security Directive (NIS 2)

Implementing and enforcing the European Cybersecurity Standard with Belden

The European Union's Network and Information Security Directive (NIS 2) first took effect in January 2023. It extends the minimum requirements for network and information security of the first version of the NIS Directive (established in 2016) and must be shifted into national law in European Union (EU) member states by Oct. 17, 2024.

Despite the regulation, there are still significant differences in how cybersecurity measures are implemented and enforced among member states. NIS 2 intends to harmonize and align cybersecurity standards across EU member states. Increasing dependency on digital infrastructureis occurring in almost all critical areas of society. For example, due to the larger attack surface created by IT-OT convergence, manufacturers are increasingly becoming targets of cyberattacks. As a result, they must be given more consideration in cybersecurity legislation.

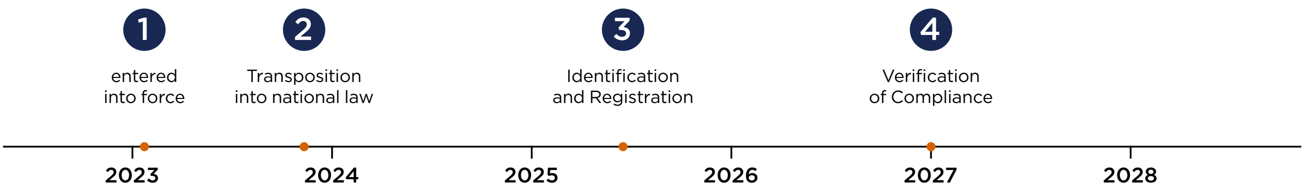
Executive Summary

While the NIS 2 Directive includes high-level risk mitigation measures to help critical companies protect their infrastructure and environments in an evolving threat landscape, it isn't specific enough to guide implementation strategies, design architectures or technology selection. Belden can help you find your path through NIS 2 and develop customized solutions that improve your cybersecurity posture – and it all begins with our Cyber Assessment Service. The white paper provides insights into NIS 2 and explains how Belden can support it.

Contents

NIS = Network and Information Security

Timeframe


1
entered into force
2
Transposition into national law
3
Identification and Registration
4
Verification of Compliance
2023
2024
2025
2026
2027
2028

1. Jan 16, 2023 NIS2 Directive takes effect
2. Oct. 17, 2024 Transposition into national law
3. April 17, 2025 Identification and registration of essential and important entities
4. 2027 Initial verification of company compliance

Noncompliance Fines

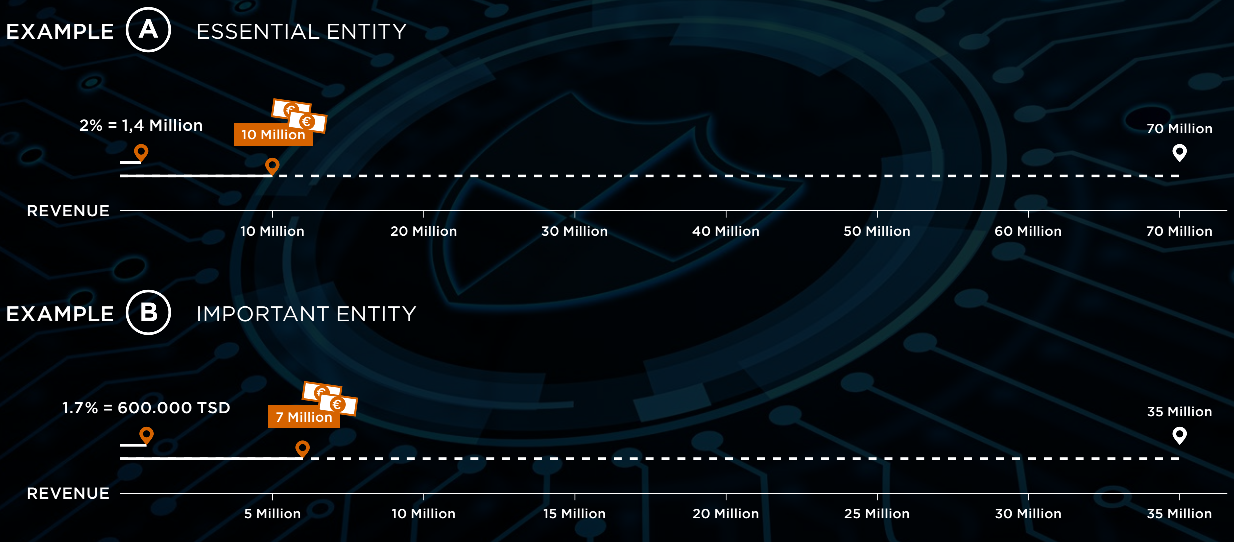
The NIS2 Directive has a structured system for sanctions. Companies that don't comply with risk management measures or reporting obligations will pay fines. This is an adapted version of the fine model of the General Data Protection Regulation (GDPR).

- essential entities: Penalties of up to EUR 10 million or 2% of global revenue (whichever's the largest)
- important entities: Penalties of up to EUR 7 million or 1.7% of global revenue (whichever's the largest)

Threshold values for affected companies

Company		Employees		Revenue		Balance Sheet
Small Company	**A**	0 – 49	and	≥ EUR 10 Mio. (max. EUR 50 Mio.)	and	≥ EUR 10 Mio. (max. EUR 43 Mio.)
Medium-Sized Company	**B**	50 – 249	and	< EUR 50 Mio.	or	< EUR 43 Mio.
Large company	**C**	≥ 250				
	D			> EUR 50 Mio.	or	> EUR 43 Mio.

Two Examples for Fine Levels



Key Take Away: In relation, the maximum penalties for companies with low revenues are significantly higher.

Scope of the directive

- Strongly expanded: applies to around 10 times as many companies in Europe
- In addition to the increase in sectors, smaller companies (from 50 employees) are also affected
- Classification is based on revenue, branch and criticality of the company

10 X MORE AFFECTED

10x times more companys affected than from NIS1

SMALL | MEDIUM | LARGE

also smaller companies (from 50 employees) affected

REVENUE | BRANCH | CRITICALITY

classification based on revenue, branch & ciritcality

Affected sectors and companies

Essential entities | Sectors with high criticality

- Energy sector
- Transportation
- Banking
- Financial market infrastructures
- Healthcare
- Drinking Water
- Wastewater
- Digital infrastructure
- Management of ICT services
- Public administration
- Space

Important entities | Companies added (expansion)

- Postal and courier services
- Waste management
- Production, manufacturing, and trade of chemicals
- Production, manufacturing, and distribution of food
- Manufacturing industry/production of goods
- Providers of digital services
- Research and development

Companies in the special public interest

- Defense equipment and IT Defense
- Value creation
- Hazardous substances

Contents of the NIS 2 Directive

The NIS 2 Directive has an impact that extends beyond EU borders. Much like the General Data Protection Regulation (GDPR), the NIS 2 Directive will set a new international standard.
CRITIS (critical infrastructure) suppliers and companies with a European location must also meet the minimum-security standards of the NIS 2 Directive. This is required to ensure **supply chain security** and prevent international disruptions from affecting services within the EU.

Registration obligations

defined in §**27** of the NIS 2 Directive **§27**

Companies must determine whether they are subject to the NIS 2 Directive and register with the respective responsible authority. Failure to register will result in fines. Companies that are classified as “essential” will be regularly inspected by the responsible authority. In the case of “important” facilities, inspections will be carried out on a random basis or following security incidents.

Verification obligations

defined in §**32** of the NIS 2 Directive **§32**

“Essential” facilities must comply with certain obligations for verification purposes, including:

- Implementing risk management measures and industry standards
- Performing audits
- Maintaining specific certificates

This is the biggest difference between “essential” and “important” facilities.

Reporting obligations

defined in §**23** of the NIS 2 Directive **§23**

Reporting obligations are tighter compared to the first NIS Directive. In the event of significant security incidents, companies must report to the responsible authority. A security incident is considered significant if it leads to serious operational disruptions or monetary losses, or if there is a possibility of this occurring. A security incident is also considered significant if a person suffers material or immaterial damage.

The following **time frame** must be observed for reporting:

I	Initial report	within **24 h**
II	Report	within **72 h**
III	Interim report	
IV	Progress report	after **one month**
V	Final report	

Continuous communication is required to assess the impact of the security incident.

Notification obligations stipulate that customers of the company must be informed of significant security incidents. Both obligations are intended to improve transparency and the ability to respond to security incidents.

Directors must be aware: **!**

Risks can’t be delegated.

Cybersecurity always needs to be a **C-Level** topic.

Director’s obligations

defined in §**20** of the NIS 2 Directive **§20**

With NIS 2, the legal framework was created to make cybersecurity a top priority. The following points must be ensured by management through the **approval, monitoring, and training obligation for managers** of essential and important entities:

- Implementation of security measures across the company
- Approval and monitoring of risk management measures
- Regular participation in training courses
- Monitoring and active participation in the implementation of compliance measures
- Proactive cybersecurity management woven into corporate culture

! **NIS 2 Compliance**

Network and information security falls within the scope of compliance under NIS 2 and must therefore also be considered in auditing as part of **business risk management.**

Risk management measures

defined in §**21** of the NIS 2 Directive §21

Risk management measures include processes and organizational measures that serve the company's network and information security.
Primary company assets should be protected according to state-of-the-art cybersecurity.
Key measures for IT and OT operations must be adapted to appropriate risk exposure, company size and potential scope of security incidents.

The following risk management measures must be taken:

a Policies risk analysis and security for information systems

- Identification and assessment of security gaps, vulnerabilities and internal cyber risks (e.g. through configurations, informal workarounds and functionality of third-party systems)
- Asset inventory through asset discovery and description of existing assets
- Regular risk analyses, cybersecurity assessments and derivations of security measures

b Incident handling

- Clear rules to handle security incidents
- Security incident response plans
- Regular assessments of security incident response plans
- Incident handling and response management that support fast response times
- Anomaly and attack detection
- Rapid forensic analysis to assess impact after attacks
- The ability to fend off malware and attackers at network boundaries

c Business continuity

such as backup management and disaster recovery and crisis management

- Secure data and networks
- Business continuity plans
- Multi-level back-up management
- Fast system recovery after an incident
- Security measures that do not negatively impact operations
- Crisis management, including an emergency plan with defined roles and responsibilities and clear communication

d Supply chain security

including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

- Selection of cyber-resilient supplier companies
- Secure network access for suppliers and service providers
- Principle of least privilege for supplier access (suppliers should only be granted the minimum level of access necessary to perform tasks)

e Security in network and information systems acquisition

development and maintenance, including vulnerability handling and disclosure

- Security measures for the acquisition, development and maintenance of network and information systems
- Vulnerability testing of third-party software
- Enforcement of security measures for IoT devices
- Disclosure and handling of vulnerabilities

f Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

- Ongoing review of cybersecurity-measure effectiveness
- Regular review of cybersecurity risk situations and associated risk exposure

1. Governance and Risk Management

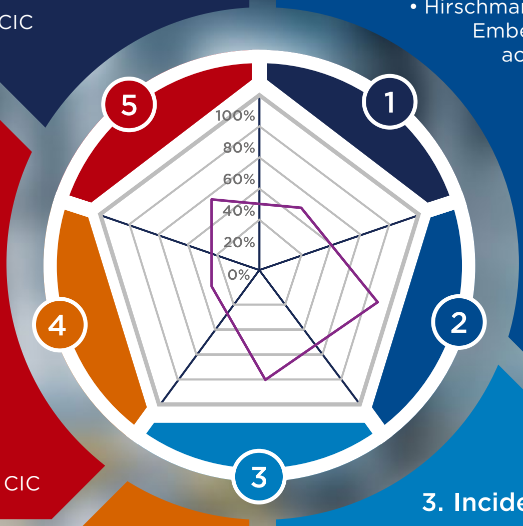
- Network and Cybersecurity Assessment Services
- Improvement of existing Networks with resilient Network Designs

+ Advisory contribution by Belden CIC

2. Cybersecurity Measures

- TXCare, Provize, Industrial HiVision & macmon NAC to design, validate, secure and manage resilient ICS networks across all levels
- Hirschmann Eagle Next-Gen Industrial Firewalls, Embedded Security Features of Hirschmann’s active portfolio (HiOS Firmware), Data Diodes and Application Access Control to protect ICS networks
- Secure Remote Access & Secure Edge Computing to build proper perimeter defenses

+ Advisory contribution by Belden CIC



3. Incident Reporting and Response

- Network and Cybersecurity Assessment Services
- Improvement of existing Networks with resilient Network Designs

+ Advisory contribution by Belden CIC

4. Collaboration and Information Sharing

- Advisory contribution by Belden CIC

5. Records and Reports that simplify Reporting Obligations of:

- Inventories
- Logical Access
- Operational Events
- Data & Information Flows
- Asset Lifecycles
- Change Control

+ Advisory contribution by Belden CIC

g Basic cyber hygiene practices and cybersecurity training

- Defense-in-depth security architecture
- Password guidelines
- Regular cybersecurity training for employees
- Updated operating systems and firmware
- Particularly strong monitoring of systems and assets that cannot be patched regularly
- Compliance with basic security norms and industry standards
- Contain potential attack impact (e.g. network segmentation, traffic filtering)
- Restrict use of system applications to the essential

h Policies and procedures regarding the use of cryptography and, where appropriate, encryption

- Secure protocols to ensure secure communication
- Encrypted transmission of sensitive information

i Human resources security, access control policies and asset management

- Visibility of users and devices in the network
- Insight into network and communication structure
- Identification and inventory of assets
- Documentation of asset properties
- Role-based access to systems
- Prevent physical unauthorized access to systems

j The use of multi-factor authentication

or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems

- Secure multi-factor authentication solutions

How Belden supports NIS 2 Implementation

Current Status of Existing Networks

The NIS 2 Directive prompts companies to implement cybersecurity standards and completely reconsider the processes required to do so. Security measures for networks and information security were not previously the focus in industrial environments, but rather system availability and efficiency. This not only results in the difficulty that numerous security mechanisms do not exist, but also that updating the systems with corresponding specifications is a challenge. Due to the long lifecycles of industrial control systems and machines, existing programming is often old and poorly documented. In some cases, available computing power is not sufficient for modern cybersecurity solutions. In addition, most OT networks have significant shortcomings in terms of inventory and visibility. Network devices and endpoints are not only partially unknown but also lack visibility of vulnerabilities and log data.

Product and Service Solutions

From the I/O block to the cloud, Belden offers many hardware and software solutions to build secure and resilient networks. The intuitive and flexible network and security solutions help organizations across a wide range of industries to implement cybersecurity measures, reduce network complexity, strengthen cyber resilience and ensure data integrity.

For OT networks, some of the required cybersecurity standards are completely new territory and there is a lack of specialists to implement them.

Belden continuously extends their product and development lifecycle certifications and work with a wide range of common standards and frameworks (e.g. IEC 62443, DNV and EN 61580).

The certifications can be found on the website.

Cyber Assessment Service

Belden offers a comprehensive cyber assessment service to collect and remediate the most impactful cyber risks of industrial environments. This results in a dedicated cyber-scoring, provisioning of a detailed remediation guide and a preliminary solution design to improve the risk posture with the help of Belden's technologies and services.

§ **Helps to comply with the following NIS2 articles:** 21a 21b 21c 21d 21e 21f 21g 22 23 24 25 29 30

The effectiveness of taken security measures are evaluated and gaps get identified to:

- Identify and document internal and external threats
- Identify risk exposure and potential mission impacts
- Identify and prioritize risk responses

The Cyber Assessment Service is intended to facilitate the long-term transfer of Belden's industrial expertise to the respective company and the development of internal know-how and security expertise. Because cybersecurity is constantly evolving, regular cyber assessments are important. Instead of infrequent or informal checks, Belden recommends a compliance program designed around continuous compliance. This approach proves to be more cost effective and identifies risks sooner. One approach is to take annual assessments and break them into smaller parts such as quarterly.

Belden's Cyber Assessment Service supports the following NIS 2 risk management measures:

Policies on risk analysis and information system security

- Assessing the effectiveness of risk management
- Planning the implementation of all the directive's risk management measures

Backbone Equipment and Network Management

Belden offers various tools to plan, configure and administer networks and network components. These are tailored to the needs and conditions of different industries to provide first-class connectivity across the backbone, aggregation and access layers of mission-critical industrial networking environments.

TXCare

For harsh environments – especially energy, transportation, mining and oil and gas industries – the XTran networking solution offers MPLS-TP backbone technologies.

XTran network structures can be planned and managed with TXCare. Thanks to SNMP-based monitoring, the software can also manage hardware components from other manufacturers.

In addition, XTran interface cards connect legacy systems that are frequently encountered in OT environments.
In existing backbone networks, asset discovery and all configurations can be managed via TXCare.
Another central component is traffic engineering.
Each network application is assigned a priority and corresponding bandwidth so that mission-critical processes can always be maintained.
XTran and TXCare comply with ISA 99, IEC 62443-4-1 and IEC 62443-4-2.

Furthermore, RFC 5920 is used as reference to protect the backbone network against common attack scenarios to follow "Security-by-Design" principles. All traffic passing over a link is encrypted in compliance with IEEE 802.1AE, utilizing 128- or 256-bit AES keys to ensure that the backbone can operate securely on the management, control and data plane.

Provize

Belden's PROVIZE enables efficient planning and configuration of aggregation and access layers of industrial networks – clearly arranged and adapted to the purpose of the network.
With just a few clicks, network segmentation can be set up or device requirements can be stored.
The PROVIZE Planner offers a network overview and various tools to reduce network complexity in day-to-day operations.

HiVision

HiVision is a network management tool that is used for the operation of Hirschmann hardware operating mainly on the aggregation and access layer. Hirschmann offers switches, routers and firewalls for industrial environments. HiVision enables network mapping, identification and extensive field-level monitoring capabilities.

All assets are documented in the application.
This visibility is an important first step for risk analysis and the development of security concepts for information systems.
The software can also be used to ensure the secure commissioning of devices. It provides real-time performance data for devices.
In addition, multi-configuration is possible for all devices or device groups.

TXCare Provize HiVision

§ Helps to comply with the following NIS2 articles: 21a 21b 21c 21d 21e 21f 21g 22 23 24 25 29 30

Belden’s backbone equipment and network management solutions support the following NIS 2 risk management measures:

Policies on risk analysis and information system security:

- Asset management
- Network monitoring

Incident handling:

- Detection and diagnosis of network failures
- IT forensics and event logs

Business continuity:

- Installation of redundancies
- Secure connection of legacy systems
- Traffic engineering

Basic cyber hygiene practices and cybersecurity training:

- Network segmentation
- Configuration hardening of device requirements
- Reduction of network complexity

Industrial Ethernet Switches

Infrastructure components play a significant role in OT network security, reliability and efficiency. Our industrial Ethernet switches run with the Hirschmann Operating System (HiOS), which provides built-in security features and a way to connect further industrial cybersecurity solutions.

§ **Helps to comply with the following NIS 2 articles:** 21a 21b 21c 21d 21e 21f 21g 22 23 24 25 29 30

HIRSCHMANN
A **BELDEN** BRAND

Belden's Hirschmann is a technology and market leader for industrial Ethernet switches. They're made for harsh environments and ensure seamless communication between various control systems, devices and sensors.

Belden's Industrial Ethernet Switches provide support for the following NIS 2 risk management measures:

Incident handling:

- Effective monitoring and visibility of network traffic
- Port security
- Denial of Service protection
- Dynamic ARP inspection
- DHCP snooping

Business continuity:

- HiOS enables high availability and redundancy, ensuring uninterrupted network operation with link aggregation control protocol (LACP), media redundancy protocol (MRP), spanning tree protocol (STP) and loop protection
- Redundant power supplies and security status indicators ensure hardware reliability

Basic cyber hygiene practices and cybersecurity training:

- Segmentation of OT networks (VLAN support, private VLANs)
- Audit trails and persistent logging

Policies and procedures regarding the use of cryptography and, where appropriate, encryption:

- SSH and HTTPS
- MACsec (IEEE 802.1AE) *

Human resources security, access control policies and asset management:

- **HiOS** supports access control mechanisms, including:
  - » IEEE 802.1X authentication
  - » TACACS+ *
  - » MAC address filtering
  - » Role-based access control
  - » IP access restriction
  - » Management VLAN
- Traffic filtering and control

* available as a software update in 2025

Network Access Control

Network access control is a central element of a holistic security concept and a powerful tool for implementing several of the risk management measures of the NIS2 Directive. Our NAC solution provides granular access authorization through role-based access control and explicit identity management. In combination with efficient authentication and authorization procedures, this ensures secure access to IT and OT networks.

§ **Helps to comply with the following NIS 2 articles:** 21a 21b 21c 21d 21e 21f 21g 22 23 24 25 29 30

With macmon NAC, Belden offers a software solution for network access control (NAC). In addition, macmon NAC enables continuous access monitoring across all users, network devices and endpoints.
This allows network visibility and implementation of asset management.

Belden's Network Access Control solution can specifically support the following NIS 2 risk management measures:

Policies on risk analysis and information system security:

- **Visibility** of all assets and consideration for risk analyses
- **Monitoring** users and devices on the company network

Incident handling:

- **Storage of network events** for 60 to 90 days
- **macmon NAC Past Viewer** collection and structuring of network events over a long period of time (up to several years)
- **IT forensic analyses** with log data
- **Use for documentation of reports** within the scope of reporting and verification obligations
- **Define reactions and policies** on how to handle certain events (e.g. trigger tickets, alerts, emails to administrators, execute certain scripts, encapsulate a field-level zone from the rest of the network for a certain period of time)

Supply chain security:

- Secure temporary network access via **macmon NAC Guest Service** for suppliers and service providers with restricted access rights

Basic cyber hygiene practices and cybersecurity training:

- **macmon NAC Compliance:** enforce security policies
- **macmon NAC VLAN Manager** for uncomplicated network segmentation
- High availability options with **macmon NAC Scalability**

Human resources security, access control policies and asset management:

- **Granular access management** for users and devices with Network Access Control

Industrial Firewalls

Firewalls contribute to maintaining operations by securing network boundaries from attackers and malware. Belden offers hardware solutions specifically for industrial security, such as our robust industrial firewalls.

§ **Helps to comply with the following NIS 2 articles:** 21a 21b 21c 21d 21e 21f 21g 22 23 24 25 29 30

HIRSCHMANN
A **BELDEN** BRAND

Hirschmann includes various Layer 2 and Layer 3 firewalls in its portfolio, including industrial firewalls with industrial protocol deep packet inspection (DPI) and routing functionalities.

Hirschmann's implementation of DPI moves beyond signatures to block traffic that does not conform to the protocol specification to provide protection against zero-day attacks. The industrial firewalls can be used to implement the zone and conduit model for network segmentation. They also provide micro segmentation for a last line of defense for PLCs and controllers by only allowing certain commands, services and function codes by authorized workstations for changes to control logic.
In this way, the potential impact radius of intruders or malware can be restricted. The firewall solutions provide round-the-clock network edge protection. By monitoring data traffic and using various encryption techniques, Belden's industrial firewalls enable secure communication in OT networks.

Belden's firewall solutions can specifically support the following NIS 2 risk management measures:

Incident handling:

- Security incident management and response
- Mitigation of cyberattacks
- Inspection of SCADA logs
- Defense against malware and attackers at network boundaries

Business continuity:

- Protection of network boundaries
- Setting up zones and control systems
- Separating functional areas or production sub-sections

Policies and procedures regarding the use of cryptography and, where appropriate, encryption:

- Encrypted data traffic in the network

Data Diodes

Data diodes are network components that function as unidirectional network appliances. The singular data flow protects networks from external cyber threats. Data diodes securely transfer Ethernet data to the public internet without putting the system at risk.

§ **Helps to comply with the following NIS 2 articles:** 21a 21b 21c 21d 21e 21f 21g 22 23 24 25 29 30

Hirschmann's Rail Data Diode secures mission-critical Ethernet networks through guaranteed one-way data traffic, while also transferring data out of the secure part of the system in a highly controlled, deterministic manner.

Belden's data diodes specifically support the following NIS 2 risk management measures:

Policies on risk analysis and information system security:

- Network component to gain control of network communication
- Securing transition zones with different security standards
- Ensures high security for mission-critical Ethernet networks

Incident handling:

- Protection from external cyber-attacks by unidirectional data flow

Business continuity:

- Extremely robust network components that resist harsh environments and weather conditions

Basic cyber hygiene practices and cybersecurity training:

- Eliminate access to paths into the secure part of the network

Secure Remote Access

To reduce downtime and related costs, companies must be able to react fast. When a certain issue appears, authorized technicians and service providers should be able to connect to a specific machine remotely. Remote access can be used to troubleshoot or perform routine maintenance without having to be onsite. This not only reduces travel costs but also keeps up with Industry 4.0 security and maintenance requirements. Regardless of its advantages, remote access can also be a gateway for cyberattacks if it isn't integrated in a secure way.

§ **Helps to comply with the following NIS 2 articles:** 21a 21b 21c 21d 21e 21f 21g 22 23 24 25 29 30

BELDEN HORIZON™

Belden Horizon is an industrial remote connectivity and edge orchestration software platform that's engineered for secure mission-critical industrial processes. It offers streamlined, secure access for remote equipment from anywhere at any time. With multi-user and multi-project-based access, it's possible to collaborate and work from different sites.

The ability to establish role-based access for users in different operation zones is an important feature to ensure access while maintaining operations. Belden Horizon can be used to create a persistent data network (PDN), which is a managed remote infrastructure communication network. A PDN connects geographically dispersed assets and enables companies to access resources and field devices securely. To ensure safe data transport, the PDN uses multi-layered, defense-in-depth techniques.

Belden's Secure Remote Access solution can specifically support the following NIS 2 risk management measures:

Policies on risk analysis and information system security:

- Secure remote access to machines and resources
- Secure connection to the cloud

Business continuity:

- **Secure data transport** using multi-layered, defense-in-depth techniques
- **Monitor gateways** to troubleshoot issues

Human resources security, access control policies and asset management:

- **Access control for users and devices** on the local network, at the edge and in the cloud
- **Role-based user and device access**

Policies and procedures regarding the use of cryptography and, where appropriate, encryption:

- End-to-end encryption
- 256-bit AES encryption

The use of multi-factor authentication:

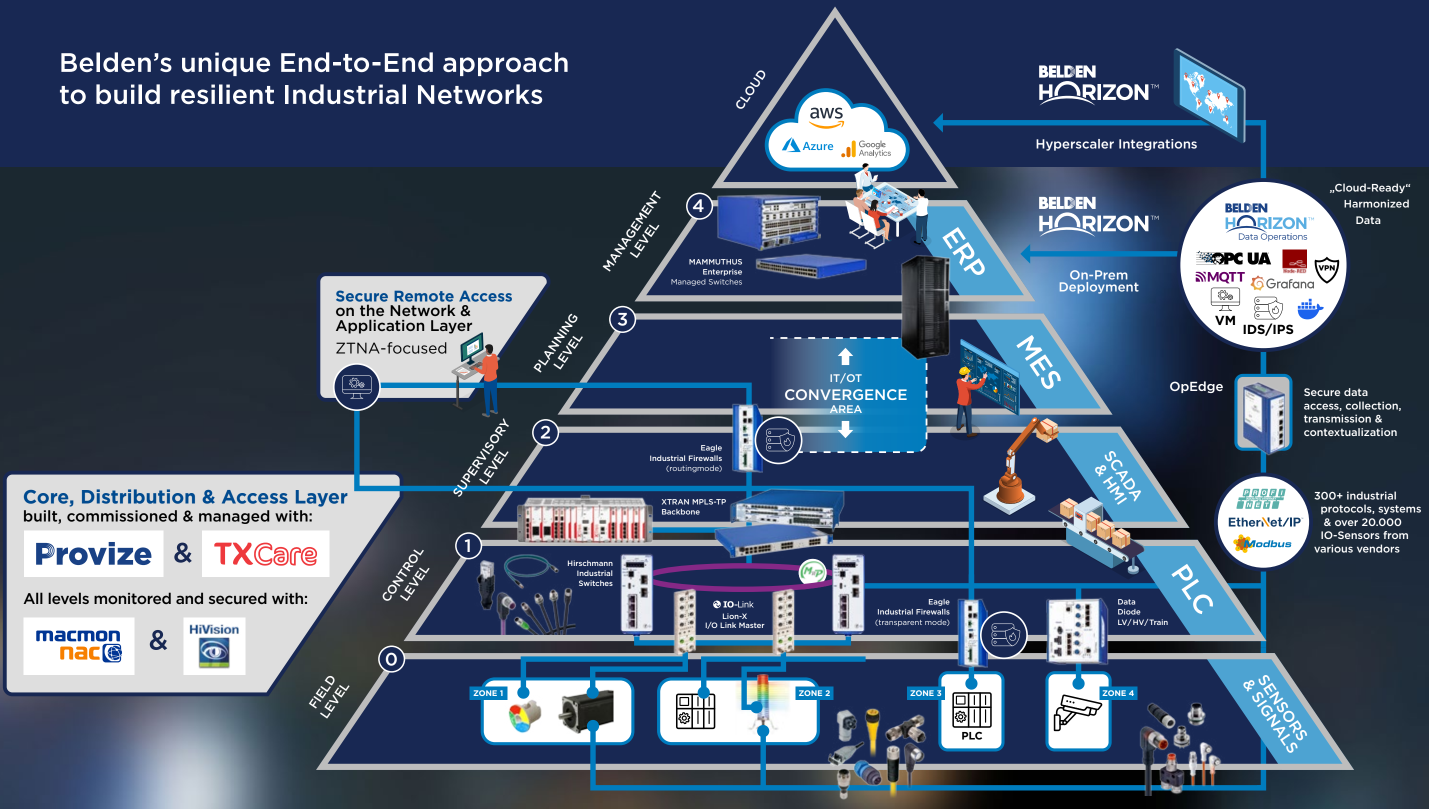
- Token-based two-factor authentication
- Built-in multi-factor authentication capabilities that utilize user-device-agent-dependencies

An Overview of Belden Solutions

Whether it’s protecting critical assets at the data source on the field level or securing communication pathways across the control, operations, and enterprise layers, Belden’s comprehensive product portfolio provides robust, adaptable solutions.
From industrial firewalls, data diodes and secure remote access to Network and Application Access Control and network visibility tools, our technology safeguards industrial environments through every layer of the Purdue Model. As we help organizations bridge their IT/OT networks, our industrial networking products enable resilience, compliance with regulations, and the secure convergence of operational technologies with cloud-based systems.

Belden ensures that organizations can confidently remediate their risks and strengthen their cybersecurity posture, from the shop floor to the top floor.

Belden’s unique End-to-End approach to build resilient Industrial Networks



Secure Remote Access on the Network & Application Layer
ZTNA-focused

Core, Distribution & Access Layer
built, commissioned & managed with:
Provize & TXCare

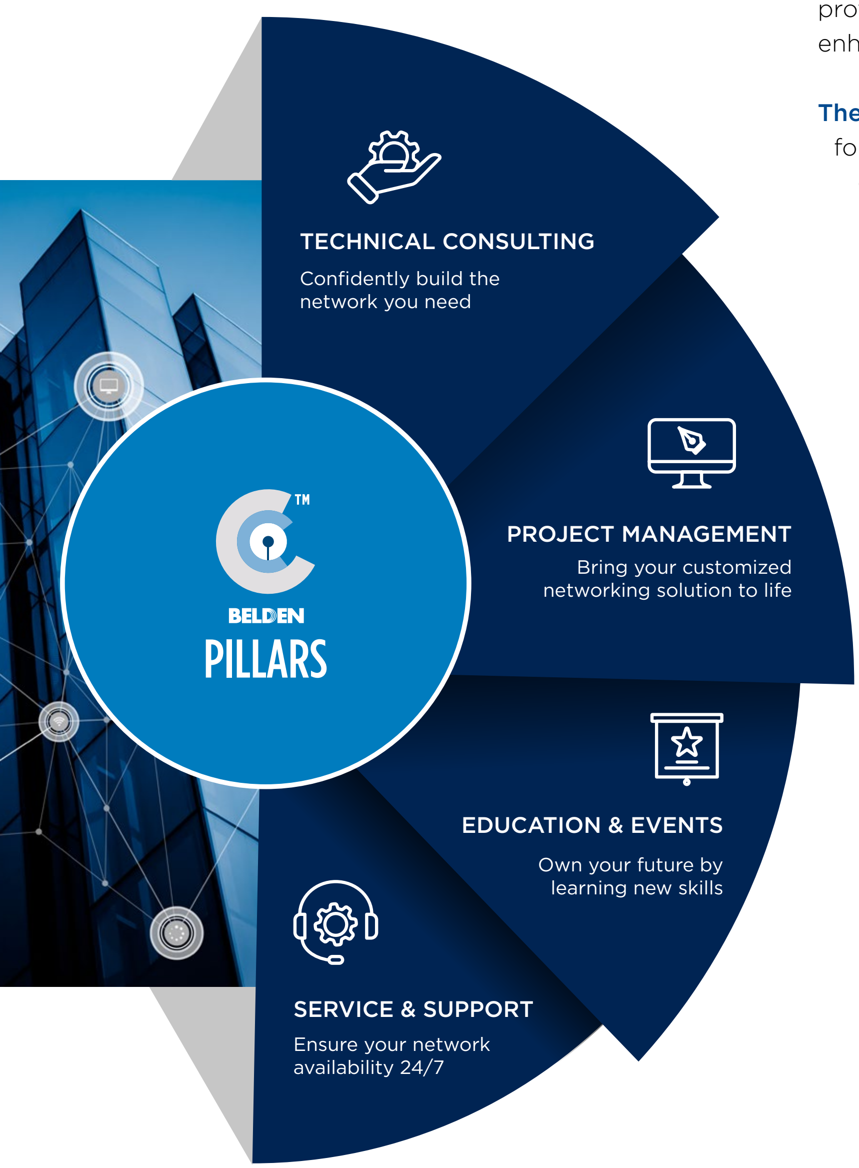
All levels monitored and secured with:
macmon nac & HiVision

Belden is able to meet client needs at every touchpoint in their cybersecurity journey.

From the data source on the field level, up to the cloud and across all levels of industrial networks.

Conclusion

The scope of the NIS2 Directive is comparable to the General Data Protection Regulation (GDPR), with a significantly expanded range of affected companies. To implement the required security measures associated with the NIS2 Directive, swift action is required across many companies – even if they aren't sure how to begin or what to do.


TECHNICAL CONSULTING
Confidently build the network you need
PROJECT MANAGEMENT
Bring your customized networking solution to life
EDUCATION & EVENTS
Own your future by learning new skills
SERVICE & SUPPORT
Ensure your network availability 24/7
BELDEN
PILLARS
TM

As they prioritize implementation, companies impacted by this directive should seek partners with the expertise to guide these changes and ensure compliance.

Belden's Customer Innovation Centers™ (CIC) can guide and support this journey. Belden's mission is to accelerate the design and implementation of robust, reliable and secure industrial networks that provide the data and insights necessary to drive enhanced business performance.

The convergence of OT and IT offers big potential for businesses. However, to leverage this potential, companies must overcome numerous challenges to achieve seamless and efficient connectivity between OT and IT systems while maintaining cyber- resilience. In OT environments, the risk management strategies required by the NIS2 Directive often need to be rethought.

Belden possesses the expertise to implement these measures while simultaneously ensuring business continuity. Belden's technical consulting is centered around close collaboration with customers to design, deploy and validate tailored-made solutions that address the specific needs of each business.

Belden experts engage in an iterative process to solve complex network challenges, optimize existing infrastructure and guide transitions to new standards. Belden provides local support and extensive market expertise in mass transit, discrete manufacturing, process automation, energy and smart buildings.

OPTIMIZE MODERNIZE AUTOMATE SECURE

Belden's CICs: Defining the roadmap for your digitization journey

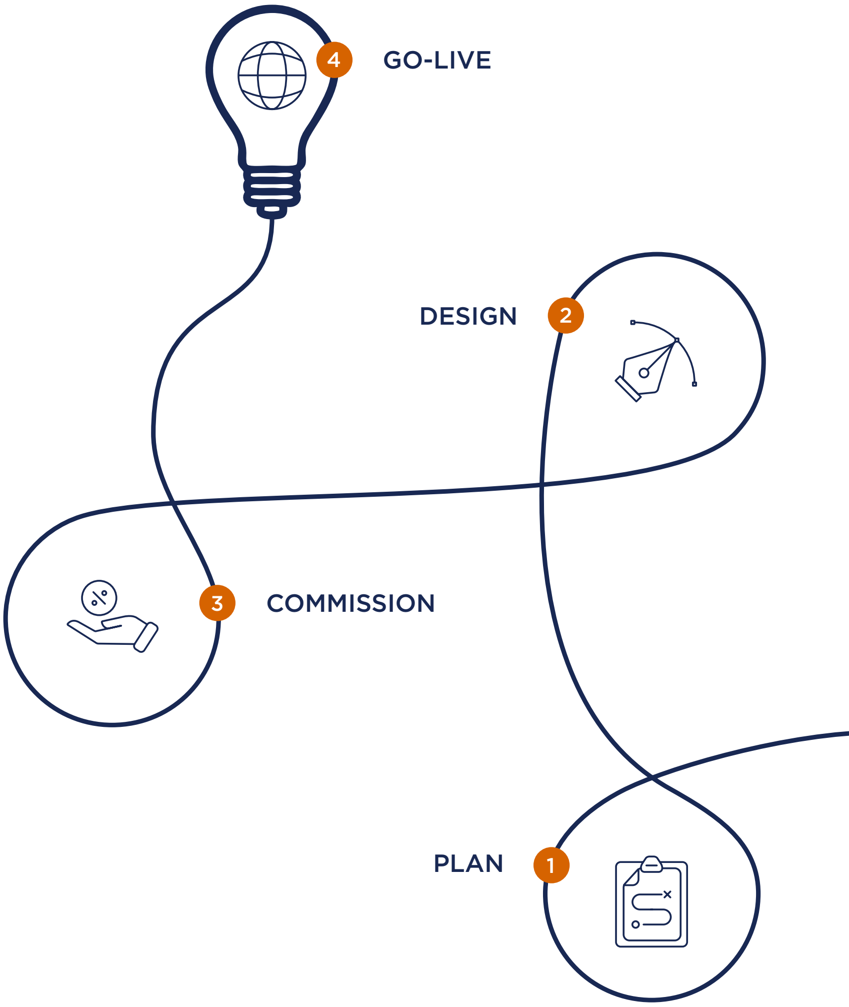
BELDEN Customer™ Innovation Center

We design and validate customized network solutions that make your digital journey simpler, smarter & more secure.

Belden offers technical demos, proof of concepts and validation testing to enhance the customer's understanding of the features and capabilities that are possible. These capabilities demonstrate how the solutions can be applied in specific use cases, including IIoT connectivity and industrial cybersecurity.

Belden supports companies in bringing customized, futureproof networking solutions to life, guiding them step by step from planning to implementation. To complete the process, Belden offers training and education to develop the necessary know-how and skills to stay ahead of technological developments and manage day-to-day needs of company networks.

Belden's support services include corrective, preventive and predictive measures to ensure network health, performance and reliability. With the expertise to prepare companies for NIS2 compliance, Belden lays the foundation for meeting future requirements.



About Belden

Belden Inc. delivers the infrastructure that makes the digital journey simpler, smarter and secure. We're moving beyond connectivity, from what we make to what we make possible through a performance-driven portfolio, forward-thinking expertise and purpose-built solutions. With a legacy of quality and reliability spanning 120-plus years, we have a strong foundation to continue building the future. We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia, and Africa.

For more information, visit us at:
www.belden.com

and follow us on **Linkedin, Facebook** and **X/Twitter**