The NIS2 Directive in Practice

Organizational and technical recommendations

GoodAccess

Table of contents

NIS2: evolution or revolution?

Today's society depends on information technology so much that it's hard to imagine we could function without it at all. Power industry, water supply management, banking, transportation, and a number of other fields and industries all rely heavily on IT for their functioning.

But more and more often, these critical services find themselves targeted by cyber threats, whether for money, political gain, or a show of strength.

This makes the need for systematic cyber protection greater than ever before.

NIS2 DIRECTIVE OF THE EUROPEAN UNION

The NIS2 (Network and Information Security 2) Directive of the European Union introduces strict requirements that impact a larger number of organizations than its predecessor (known as the NIS Directive).

The increased number of obligated entities and the scope of new technological and organizational requirements both show the tremendous significance of NIS2. Furthermore, its actual implementation will be so complex that it will require a joint collaboration of lawyers, consultants, and IT vendors.

Every EU member state should transpose the Directive to its national legislation by October 2024, which leaves little time to prepare. Deploying a functioning cybersecurity system that is compliant with the legal requirements can take months, even years. And, it will come with major costs in both investment and operation.

This text describes the technical and organizational requirements that organizations will have to meet and outlines the potential of the zero-trust approach as a means of achieving compliance.

2024: A crucial year for cybersecurity in Europe

The European Union is not new to battling cyber threats. In 2016 it issued the original NIS Directive to standardize the cyber protection of the most sensitive sectors.

COMPLEX REGULATION

In 2023 the Directive was succeeded by NIS2, whose aim is to create a high cybersecurity standard across the EU. Unlike its predecessor, NIS2 represents a much broader and more complex regulation, as it requires not only the protection of all systems that are essential for the society, but also the security of all systems involved in the providing of important services.

NEW NIS2

EU member states will adopt the Directive by transposing it to their own laws. These will represent specific and legally binding norms adjusted for the unique context and requirements of each nation. These laws should become effective by the end of 2024.

Newly, the scope of NIS2 will include mid-size and large organizations from 18 sectors. They will have to implement cybersecurity risk-management measures, i.e. deploy new technologies and implement security procedures.

NIS2 covers the following obligated sectors:

- ENERGY
- HEALTH
- BANKING
- TRANSPORT
- FINANCIAL MARKET INFRASTRUCTURES
- DRINKING WATER
- WASTE WATER
- PRODUCTION
- DIGITAL INFRASTRUCTURE
- ICT SERVICE MANAGEMENT
- PUBLIC ADMINISTRATION
- SPACE
- POSTAL AND COURIER SERVICES
- WASTE MANAGEMENT
- MANUFACTURE
- PRODUCTION AND DISTRIBUTION OF CHEMICALS
- PRODUCTION AND DISTRIBUTION OF FOOD
- MANUFACTURING
- DIGITAL PROVIDERS
- RESEARCH

What changes does NIS2 bring?

NIS2 represents a significant step towards strengthening cyber resilience in the EU, reflecting the evolving threat landscape and increasing importance of digital services for the functioning of society and internal market. The NIS2 Directive is driven by five main objectives.

Broader scope

NIS2 expands the scope to include more sectors and services categorized as either essential or important organizations. To the original scope of 7 industries are added 8 new, including providers of public electronic communications networks and services, digital services (social networking services, data center service providers), waste management, and others. See **this factsheet** published by the Commision to learn more.

Stricter requirements

NIS2 introduces more stringent security requirements, including supply chain security, business continuity, crisis management, cybersecurity training, access control policies, use of MFA or continuous authentication methods, and others. If you want to dig deeper into these requirements, check out our article where we break down **10 minimum cybersecurity risk management measures** of the NIS2 directive.

Stricter penalties

NIS2 introduces new penalties by increasing the upper limits of financial sanctions and by implementing non-monetary penalties and criminal sanctions for the management.

Enhanced supervision

There will be an enhanced supervision, incident reporting obligations, and fines for non-complying with the NIS2 directive. Management of the affected entities can be held personally accountable for legal infringements.

EU-wide cooperation

The Directive sets the basis for establishing the European Cyber crises liaison organization network (EU-CyCLONe) that should be a central point for coordinated action against large-scale cybersecurity incidents and information/experience sharing.

How to determine if your organization falls under NIS2's scope?

The primary method for determining whether a private or public organization falls under the regulation of NIS2 is the simultaneous fulfillment of two requirements:

Importance

The entity provides services mentioned in at least 1 of the sectors listed in Annex I or Annex II of the Directive.

Size

Companies fall under the scope of NIS2 if they meet the definition of large or medium-sized enterprise. Generally, the NIS2 size threshold for enterprises is 50 employees, and an annual turnover of 10 million Euros or a balance sheet of 10 million Euros. Determining whether the organization fulfills the size condition can be a bit more complicated, as it requires assessing the relationship with the so-called interconnected enterprises.

However, there are exceptions and entities providing selected essential services will have to comply no matter their size (e.g. DNS service providers). See the General provisions of the Directive, (7), and Annex I and II for further guidance.

Once you have determined you must comply with the NIS2 directive, the next step is to determine if you fall under the essential or important entities requirements.

How to determine whether my organization is an essential or important entity?

NIS2 classifies organizations as either an essential entity or important entity as follows:

Essential entities – Large companies (more than 250 employees, annual revenue of at least €50M, or an annual balance sheet total of at least €43M) listed in Annex I (sectors of high criticality).

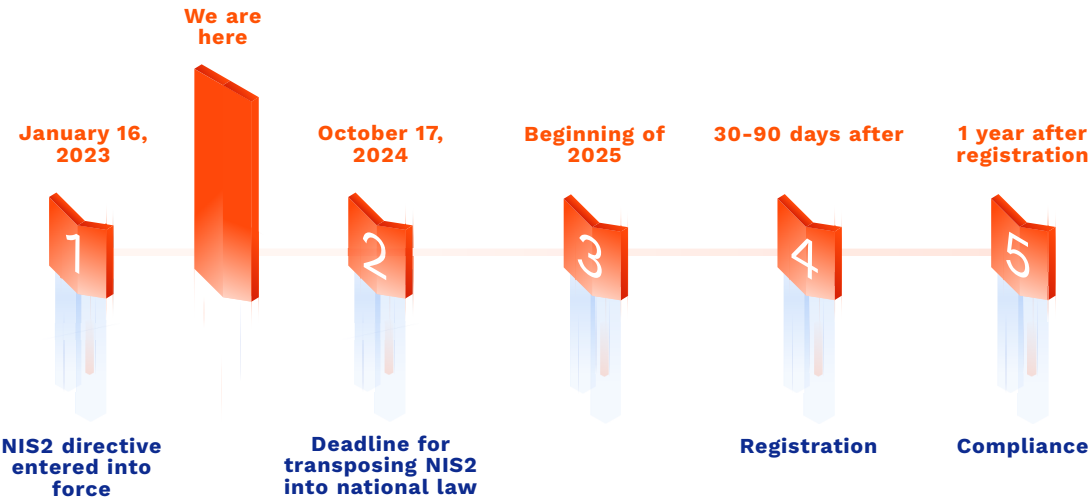
Important entities – Medium-sized enterprises (at least 50 employees or an annual revenue or balance sheet total of at least €10M) operating in industries listed in Annex I (high criticality sectors), or large or medium-sized enterprises listed in Annex II (other critical sectors).

PENALTIES

The primary distinction between essential and important entities lies in the strictness of supervision and the severity of penalties for non-compliance. Essential entities will be subject to proactive supervision to ensure adherence to NIS2 requirements. In contrast, important entities will undergo ex-post supervision, meaning they are monitored reactively. Authorities can impose sanctions if they determine that an entity is not compliant.

Also, national authorities may also classify entities as essential or important regardless of the NIS2 criteria. For example, if a service disruption could significantly impact public safety, security, or health, authorities might assign these designations.

What is the timeline of NIS2 compliance?



Once the organization determines it is a subject of regulation, it should register itself to the national authority register of obligated entities. Please note that the period for registering the obligated entity may vary depending on national law specifics.

Regulated service providers will have **a year to implement the technical and organizational measures** in compliance with the new NIS2 Directive, i.e. the national laws based on it.

However, organizations shouldn't delay preparation for NIS2 for two main reasons.

REQUIREMENTS

NIS2 is introducing many obligations and technical requirements. These could take a long time to implement in larger, but also mid-sized organizations, especially if it is new to implementing complex cybersecurity countermeasures.

IMPLEMENTATION

The implementation can also come with significant initial and operational costs. Organizations will have to allocate sufficient resources and find or train experts to handle cybersecurity matters in the company.

The whole process can take several months, even years, especially if the organization belongs in the essential category.

Who is responsible for NIS2 compliance in the organization and what sanctions are there for violations?

Regulated entities should have staff members or suppliers to fulfill security roles. The purpose of these roles is to develop and manage cybersecurity in the organization, oversee its status, design and implement security measures, and communicate cybersecurity to the management.

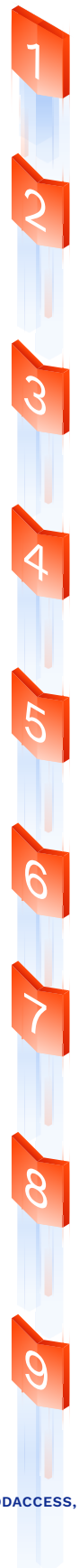
The organization's management is held personally liable for creating these roles as well as for allocating resources for cybersecurity, integrating security principles into all processes, and more. In other words, NIS2 requires the management to actively participate in cybersecurity management and threatens penalties for failure to do so.

The maximum fine that can be issued is equal to 2% of annual turnover in the case of essential entities and 1.4% in important entities.

Besides fines, continual violation of the Directive's requirements may result in the suspension of the management or revoking cybersecurity certification.

How to prepare for NIS2

Obligated entities must take several steps to achieve compliance with NIS2. The list below is far from definitive, but it gives a basic idea of how a cybersecurity manager approaches the task.



1. Understands the organization's context and business goals.
2. Helps take inventory of all of the organization's assets, determining their value and role in providing the regulated service.
3. Surveys the current state of cybersecurity management in the organization.
4. Establishes a risk management process and helps identify and assess the risks depending on the type of organization, ideally using data from MITRE ATT&CK.
5. Drawing on the risk analysis, compiles a response plan and a declaration of applicability (an overview of cybersecurity measures).
6. Based on the previous steps, they can help create the organization's cybersecurity strategy.
7. Creates an implementation plan of the cybersecurity measures.
8. In essential entities, cooperates with the cybersecurity architect and defines the final security architecture of the organization.
9. Takes part in the implementation and testing of security processes (e.g. incident management, access control, etc.).

10 Helps the organization choose suitable technology partners and vendors of security solutions (end-point protection, ZTNA, log management, SIEM/SOAR, etc.).

11 Communicates with national authorities about regulations.

12 Helps organize cybersecurity training.

13 Reports to the organization's management.

Cybersecurity management is a never-ending process. The highest costs come at the beginning of the project, i.e. when the organization is implementing new processes and purchases and deploys new technologies. However, once its cybersecurity matures, the costs can be expected to decrease.

Technologies to meet NIS2 requirements

The new cybersecurity legislation requires regulated entities to deploy new technologies. Though the final requirements will be listed in the national transpositions, NIS2 itself already provides clues as to which technologies essential and important entities will have to implement.

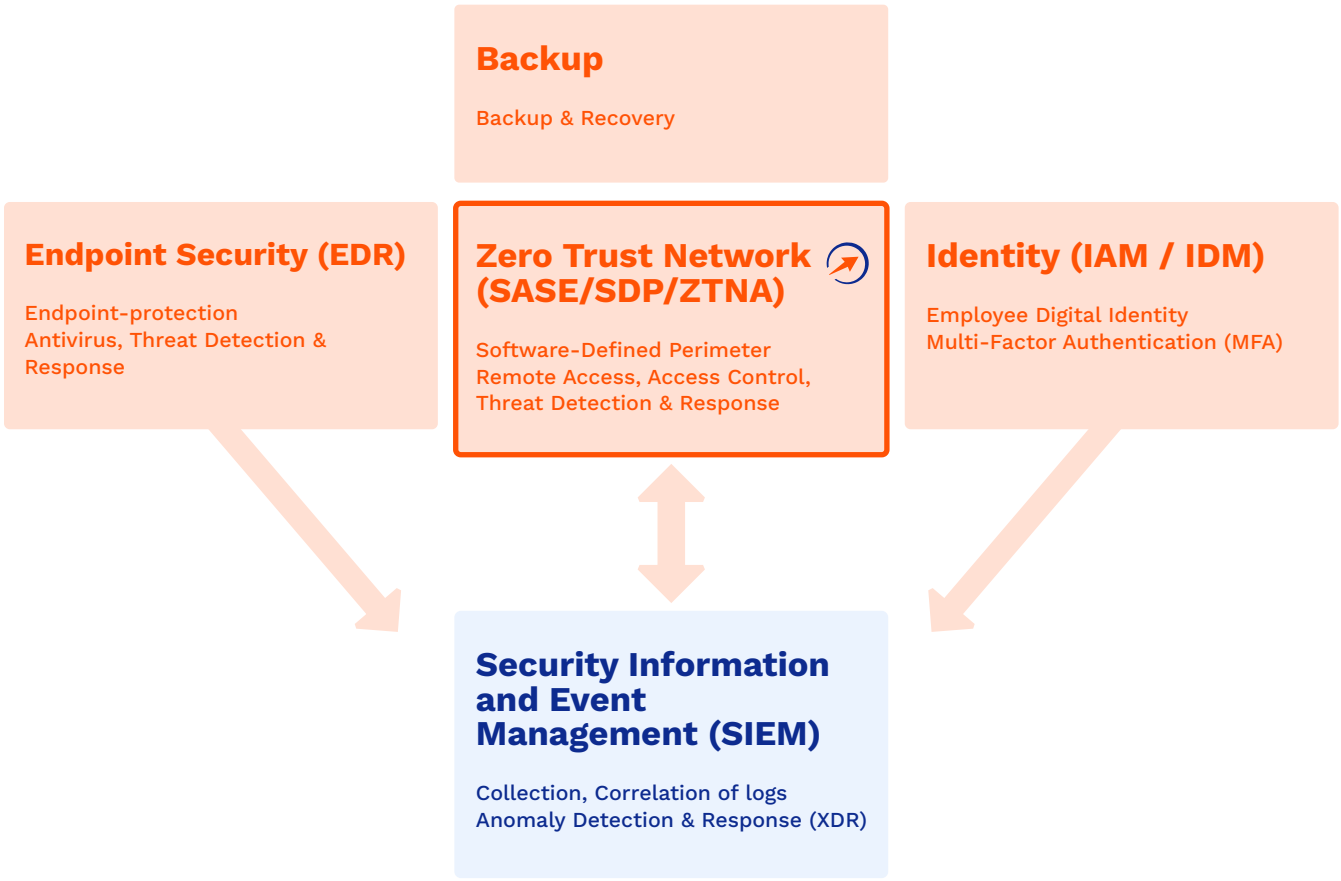


Fig. 1: Technologies to meet NIS2 requirements

On top of these technologies it is worth mentioning MSSP (managed security services provider) services. These vendors can perform risk analysis, create ISMS, set up processes, or provide cybersecurity manager roles as an outsourced service.

One of the basic protective mechanisms that the NIS2 Directive specifically mentions is the zero trust principle. The following section explains what zero trust is and how it can be implemented in an organization to meet the requirements of the Directive.

What is zero trust

Zero trust is a security model whose goal is to reduce cybersecurity risk and eliminate vulnerabilities. The phrase “zero trust” refers to the practice of treating every part of company infrastructure as a potential threat. In other words, all network traffic is considered potentially malicious and thus cannot be trusted.

Every user, device, and network connection must be authenticated and verified before being granted access to applications and data.

Implementing zero trust principles can significantly increase the organization’s cybersecurity posture and reduce the risk of security incidents, unauthorized access, and lateral movement in the IT infrastructure.

Solutions that introduce the principles of zero trust will be crucial to achieving NIS2 compliance. Below is a description of the GoodAccess zero trust solution with regard to NIS2 compliance

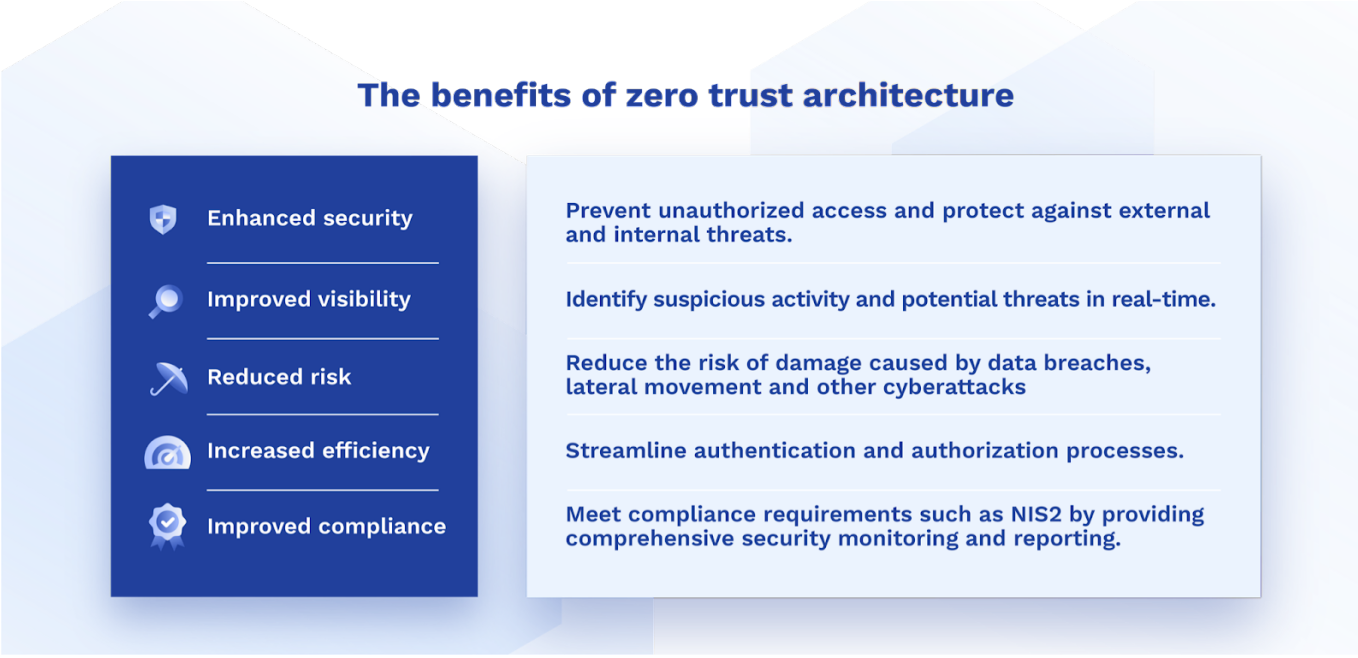


Fig. 2: Benefits of zero trust architecture

GoodAccess' zero trust architecture and NIS2

GoodAccess is a SaaS tool that enables organizations to quickly integrate zero trust principles into their security architecture without major changes to their existing infrastructure. In this way they can easily secure access to their critical resources; i.e. networks, systems, and data, from anywhere and at any time.

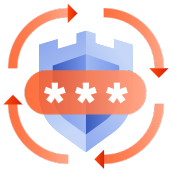
The GoodAccess zero trust platform aggregates several technologies that help meet the technical requirements of NIS2. These key elements are:

Device posture check

A mechanism that checks whether devices (computers, smart phones, tablets, etc.) conform to pre-set security policies. Examples include an active and up-to-date antivirus, firewall, operating system with the latest update, disk encryption, enabled biometrics, and more.

Identity management (MFA)

MFA is part of identity-based access control, which is an integral component of the zero trust approach. MFA can be implemented on the application level, e.g. as part of SSO, or on the network level during authentication. GoodAccess supports biometric MFA or login via an approved user device.

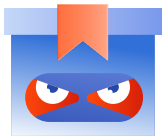


Access control

Microsegmentation allows administrators to assign access privileges on the level of user-application interaction. This minimizes the risk of data misuse and, in case of an incident, narrows down the root-cause investigation.

Access logs

GoodAccess collects gateway- and system-level access logs, which helps prevent and investigate incidents. Access to critical systems is logged on the network layer. This enables organizations to gain control over the whole perimeter, which means they are not dependent on the logging capabilities of their individual applications.



Threat detection and response

GoodAccess ensures that the only way to access a system is via one of its gateways (on-prem or cloud-based). This allows organizations to immediately deny access to a specific user or device and stop a cyber threat early.

Encryption

All communication passing between a user and data source is encrypted, which is another of NIS2's requirements for obligated entities. Encrypting sensitive files and databases adds another protective layer against potential threats, rendering data unusable even if the attacker gets hold of it.

Deploying GoodAccess

Deploying a zero trust solution usually comes with some hurdles, such as applications being incompatible with zero trust principles, difficulty of managing the solution, limited experience and expertise, low flexibility, or high costs.

The biggest problem is usually heterogeneous infrastructure, i.e. infrastructure comprising network elements from different vendors, spanning multiple cloud environments and branches, and including applications that do not support MFA and SSO. Such infrastructures make it difficult to secure user access, especially when they are using their own devices or when third-party vendors or contractors need access to critical IT resources.

Here is how the cloud-based GoodAccess solution eliminates these obstacles:

Operates on the network layer

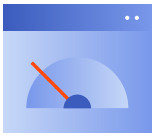
This enables it to provision authenticated access to older applications and systems that often don't support SSO and MFA. GoodAccess is also easy to integrate into the existing IT infrastructure, whether this includes identity providers, network hardware (routers), or cloud service providers (AWS, Google Cloud, MS Entra ID), and more.

Access to systems and data from anywhere

GoodAccess is a one-click application. It makes no difference whether employees are using an Android, macOS, iOS, Windows, or Linux device. They connect via a client app (agent) that handles MFA, identity verification, and device posture check. Once all these have been successfully passed, the user is granted secure, encrypted access to the company network.

Easy management of the secure environment

GoodAccess is designed to be easy to manage without deeper IT knowledge. The administrator uses a web-based interface that gives them full control of the perimeter and everything connected to it. They can manage user accounts and their privileges, define protected systems (including cloud and branch connections), monitor network activity, and device security. When a threat emerges they can disconnect the compromised device from the network and investigate the incident.



Automation and scalability

GoodAccess can be integrated with identity access management, which automates a number of routine tasks associated with user identity and account management. For example, the HR department can manage user groups and assign privileges in the IAM tool, while all their settings will automatically synchronize with GoodAccess thanks to SSO and SCIM support. This saves time, allows them to quickly respond to changing needs of the company, and reduces the risk of human error of adding/removing users and devices manually. Because GoodAccess is cloud based, it is highly scalable, so everything is only a matter of a few clicks.

Lower costs

Managing an in-house zero trust solution comes with additional investment into infrastructure and operational costs. This can be a significant financial burden for a lot of companies, not to mention keeping the system up-to-date, free of vulnerabilities, etc. All this requires a qualified IT expert to manage. However, GoodAccess is cloud-based, which means all this management overhead is placed on the vendor and the subscription model makes costs easily predictable.

How GoodAccess helps meet the technical requirements of NIS2

NIS2 provides clear guidance on technical and organizational requirements that will be largely consistent across national regulations. Although the final wording of national laws has not been determined, we can anticipate the technical and organizational measures organizations will be required to implement. For a better understanding, we can examine one of the strictest national cybersecurity laws based on NIS2—the Czech National Cybersecurity Act.

Technical measures	
Physical security	This involves the security of assets in the physical world and technical-organizational processes. Our partner ProID can unify the physical and digital identity using physical access cards and hardware tokens
Network security	GoodAccess provides authenticated network connections, network-level access control, encryption, and secure remote access from any device the employees may use. It segments the zero trust perimeter and defines critical systems as network services that cannot be accessed except through the perimeter. This isolates critical systems from the public internet and other non-authenticated network traffic.
Identity verification and management	GoodAccess fully integrates with identity providers (IAM/IDM) using SSO, SAML, and SCIM. This makes it possible to employ MFA not just on the application layer, but on the network layer as well, providing MFA even on applications that do not support SSO/SAML. GoodAccess can also be used for privileged access management (PAM) by creating a time-limited access card that grants admin access to a selected critical system and will automatically invalidate itself upon expiration.
Access privilege management	GoodAccess enables central management of critical systems on the network level, regardless of the capabilities of the critical application. Depending on the application, additional access controls may be needed within the application, which would be implemented on the application layer.

Technical measures	
Cybersecurity incident detection	This requires a combination of endpoint protection and threat detection (EDR) with network detection. GoodAccess handles basic threat detection. In some cases it may be wise to add an advanced solution for network detection and response (NDR). GoodAccess integrated with a SIEM can immediately respond to the detected threats by blocking access to a user or device to the critical resource. The user's virtual access card can be revoked manually or automatically, which is crucial for averting the cyberattack early.
Security and relevant operational incident logging	GoodAccess records security and relevant operational events on the network and gateway level. This provides a detailed overview of access attempts to the perimeter and individual resources.
Cybersecurity incident assessment	GoodAccess can be fully integrated with a SIEM. This enables additional log processing, such as event correlation with EDR and IAM logs, providing effective threat and anomaly detection on all levels.
Application security	GoodAccess protects applications by sealing them away from the public internet and unauthenticated network traffic. However, here it is necessary to perform regular vulnerability checks, regular updates, and penetration testing.
Cryptographic algorithms	In its full deployment, GoodAccess provides a secure zero trust perimeter that prevents all access to critical resources unless properly authenticated by GoodAccess. Once authenticated, all communication is encrypted on the network level. For full protection, we recommend supplementing by application-layer encryption as well (SSL/TLS, end-to-end encryption, etc.).
Regulated service availability	Can be fulfilled by technical-operational backup, recovery, and redundancy policies.
Security of industrial, control, and special technical resources	GoodAccess can be used to secure industrial, control, and other IoT resources

Conclusion

The introduction of NIS2 places regulated entities before significant technical, organizational, and legal challenges. It is clear that achieving NIS2 compliance will not always be simple. It will involve an extensive gap analysis to understand what the organization needs to do to meet the regulation, including a new strategy, technologies, adjusting internal policies, and organizational processes – all this will take much time, effort, and money.

That is why you should start as soon as possible and find partners to help you with meeting the Directive's requirements now.

If you're interested in a non-binding consultation on NIS2, or you wish to know more about the GoodAccess solution, please, contact us at **sales@goodaccess.com**.

Michal Čížek
CEO GoodAccess

P: **+420 605 264 263**
E: **michal@goodaccess.com**
W: **www.goodaccess.com**