

SOLUTION BRIEF

NIS2 Directive

Leverage Trellix® for cybersecurity resilience and compliance

What is NIS2?

Network and Information Security Directive 2 (NIS2) is an approved EU directive drafted to increase cybersecurity and resilience across the EU. It is not a framework of specific security controls, but rather a mandated continuous risk management approach that will consistently improve cybersecurity maturity, incident management, and information sharing across critical infrastructure companies and member states.

Who is affected by the NIS2 Directive?

The types of organizations affected by the NIS2 Directive are extensive, including entities providing essential services like energy, transport, banking, health, water, digital service providers, and public administration. It also encompasses entities providing important services such as postal and courier services, waste management, chemical manufacturing, ICT service providers, food production and distribution, and certain types of manufacturers. For a complete list of affected organizations, please refer to the full text of the [NIS2 Directive](#).

Why use Trellix for NIS2 compliance?

Trellix speeds up your implementation of NIS2 requirements. [Trellix Helix](#) delivers threat detection and response capabilities across information technology (IT), operational technology (OT), and the cloud to increase your enterprise visibility. Trellix Helix integrates data from Trellix sensors and 500+ third parties using prebuilt analytics to create multivector, multivendor detections and uses AI-powered automation to reduce incident response times. The complete [Trellix Security Portfolio](#) delivers the advanced security controls required to improve cyber hygiene across endpoints, servers, networks, data, cloud, and mobile devices. [Trellix Consulting Services](#) can assess your current security program against international and European standards, providing readiness assessments and threat intelligence for continuous risk analysis.

Specific compliance requirements may vary depending on member state implementation guidance, but the common thread for NIS2 compliance is cyber risk reduction and resilience. Below we outline the top five ways that Trellix, in collaboration with our partner solutions, can help you meet NIS2 requirements and manage your risk of emerging threats.

Identify your risk with Trellix Assessment Services

The NIS2 Directive mandates that organizations conduct risk assessments and adopt international or European standards such as ISO27001 or NIST Cybersecurity Framework to manage cyber risk continuously. It is important to assess your current state against one of these standards and your readiness in potential high-risk areas. Based on our experience and Trellix threat intelligence, we recommend focusing on these five key assessments.

| Trellix Services | Service Description | Related NIS2 Articles |
|--|--|---------------------------------|
| Cybersecurity Assessment | Maturity assessment against international standards and establishment of info security policies | 20.2, 21.1, 21.2a |
| Intelligence as a Service | Identify targeted threats putting your business at risk | 20.2, 21.1, 21.2a |
| Ransomware Readiness Assessment | Custom tabletop exercises to assess your ransomware risk | 20.2, 21.1, 21.2a, 21.2c, 21.2f |
| SOC Readiness Assessments | Incident Response Program Development, SOC assessment and design, and emergency IR support during a crisis | 20.2, 21.2a, 21.2b, 21.2f |
| Web Application Assessment | Assess DevSecOps processes and external applications | 20.2, 21.2a, 21.2f |

Schedule Trellix Assessment Services through your Trellix representative or at www.trellix.com.

Build your ransomware resilience

Our [Trellix CyberThreat Report](#) describes the toll of recent ransomware attacks. Ransomware is a significant threat to the entities delivering essential services governed by NIS2. High-profile attacks affect energy, transportation, public administration, and other sectors, disrupting essential services. Organizations must build a robust defense to prevent, detect, and respond quickly to ransomware attacks. In addition to Trellix Ransomware Readiness Assessments, we recommend leveraging the following Trellix solutions to close gaps in malware protection and reduce the risk of ransomware affecting business operations.

| Trellix Solutions | Solution Description | Related NIS2 Articles |
|--|--|---|
| Trellix Endpoint Security and EDRF | Advanced ransomware protection and detection on end-user systems, servers, and mobile devices | 21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j |
| Trellix IVX for Collaboration Platforms | Prevent and detect ransomware delivery from phishing emails and collaboration applications | 21.2g, 21.2j |
| Trellix File Protect | Identify ransomware hiding in storage and custom business applications | 21.2c, 21.2g |
| Trellix Network Security | Prevent and detect lateral movement and later stage ransomware techniques | 21.2e, 21.2b |
| Trellix Helix | Integrates and analyzes data across Trellix and third-party tools to accelerate detection and response to ransomware | 21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j |

To learn more about how Trellix can protect your business from ransomware, visit www.trellix.com.

Accelerate SecOps threat detection and response

One of the main goals of the NIS2 Directive is to improve incident detection and response across the enterprise. Many operators of essential services likely face common security operations center (SOC) challenges such as visibility gaps, talent shortage, and lack of automation. Our SOC and incident response (IR) assessments expose these gaps and help you design an action plan to remediate and mature the program.

From a technology perspective, Trellix Helix with integrated Trellix Wise AI reduces analyst workload and mean time to respond (MTTR) with an open platform that integrates data from Trellix sensors and 500+ third parties. We enrich the data with built-in threat intel and AI-driven automation, providing rapid detection and response across IT, OT, and cloud networks. In addition to Trellix Helix and SOC assessments, we recommend the following Trellix solutions to provide deep visibility and threat detection across the enterprise.

| Trellix Solutions | Solution Description | Related NIS2 Articles |
|--|---|---|
| Trellix EDRF and Endpoint Forensics | Provide deep endpoint visibility, malicious activity detection, and IR forensics | 21.2b, 21.2g |
| Trellix NDR and Network Forensics | Provide full network packet capture and malicious network activity detection | 21.2e, 21.2b |
| Trellix IVX for Enterprise Applications | Highly scalable cloud malware analysis | 21.2b, 21.2g |
| Trellix Helix | Integrates and analyzes data across Trellix and third-party tools with built-in threat intel, AI, and analytics to reduce MTTD and MTTR | 21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j |
| Trellix Second Sight | Proactive service that hunts for emerging threats and alerts customer to potential new incidents, greatly reducing attacker dwell time | 21.2a, 21.2b, 21.2c, 21.2d, 21.2e, 21.2f, 21.2g |
| Semperis (Partner) | Protects Directory Services and integrates with Trellix Helix for identity detection and response capabilities | 21.2g, 21.2i |

Protect your operational technology networks and systems

Many entities delivering essential services governed by NIS2 run OT systems and networks. These OT systems are critical to business resilience and are often the target for threat actors. OT faces heightened risk as security controls are often insufficient to prevent advanced threats. Additionally, OT security monitoring is typically handled separately from the IT security teams by inexperienced operators. The [Trellix Security Portfolio](#) helps secure your critical operational technology systems. Trellix Endpoint Security provides basic and advanced controls for OT systems and is certified by every major Supervisory Control and Data Acquisition (SCADA) manufacturer.

However, endpoint security alone is not sufficient protection. It's vital to have asset visibility for vulnerabilities, network security controls at the boundaries, and monitoring to detect anomalous behavior. In addition to Trellix Endpoint, we recommend leveraging the following Trellix solutions to close gaps in malware protection, provide specific SCADA asset visibility, and detect potential threats.

| Trellix Solutions | Solution Description | Related NIS2 Articles |
|--|---|---|
| Trellix Endpoint Security | Advanced ransomware protection on end-user systems, servers, and mobile devices | 21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j |
| Trellix Embedded Security | Advanced ransomware protection on end-user devices and servers in OT environments | 21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j |
| Trellix Network Detection and Response Security | Detect malicious network activity between IT and OT networks | 21.2e, 21.2b |
| Nozomi Networks (Partner), Tenable (Partner), Armis (Partner) | Discover SCADA asset details and vulnerabilities, integrate with Trellix NDR and Trellix ePO for threat detection and response | 21.2b, 21.2c, 21.2e |
| Trellix Helix | Integrates and analyzes data across Trellix and third-party tools to improve incident detection and response on OT and IoT networks | 21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j |

To learn more about how Trellix can protect your operational technology systems, please review this [case study](#).

Reduce the risk of a data breach incident

Protecting sensitive and proprietary data is getting harder. First off, data is everywhere—in customer applications, cloud storage, databases, and on personal devices. Secondly, there is the risk of compromise from external and internal threats. External APT actors are leveraging AI to generate exploits faster, which puts your sensitive customer and corporate data at risk of exposure through vulnerable applications. Additionally, there is a growing risk of insider accidental and malicious data breaches. This all increases the likelihood of a reportable compromise or loss situation. As NIS2 dictates short reporting timelines for a data breach incident, it's critical to focus on improving your data security program.

Trellix Consulting Services can jump start your data security program by aligning your business information security priorities to protection control. Secondly, Trellix DLP Discover will scan your network and repositories like SharePoint, improving visibility and classification. These will help get you started but for full protection we recommend implementing the following Trellix Data Security controls to mitigate the risk of a data breach from device to cloud.

| Trellix Solutions | Solution Description | Related NIS2 Articles |
|--|---|-----------------------|
| Trellix Data Loss Prevention (DLP) Endpoint Complete, Drive Encryption, File and Removable Media Protection | Discover, classify, and protect data loss from the endpoint; encrypt data at rest | 21.2h, 21.2i |
| Trellix DLP Network Suite | Discover, classify, and protect against data loss over the network | 21.2i |
| Trellix Database Security | Monitor and control access to sensitive information in application databases | 21.2i |
| Trellix AI Risk Dashboard | Identify and monitor AI service usage | 21.2a |
| Skyhigh Security (Partner) | Monitor and control access to sensitive information in cloud applications | 21.2d, 21.2i, 21.2j |

To learn more about Trellix and NIS2, please visit www.trellix.com or schedule a workshop with your Trellix representative.