SOLUTION BRIEF

NIS-2 Directive

How Trellix can ensure cybersecurity resilience and compliance across organizations and sectors.

What is NIS-2?

Network and Information Security Directive 2 (NIS-2) is an approved EU directive drafted to increase cybersecurity and resilience across the EU. It is not a framework of specific security controls but 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 NIS-2 Directive?

The types of organizations affected by the NIS-2 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 NIS-2 Directive.

Why use Trellix for NIS-2 compliance?

Trellix helps you meet NIS-2 requirements faster. Trellix Helix Connect unifies visibility of threats across your environment with deeper detection of threats that point tools alone may miss. Trellix Helix Connect integrates data from Trellix security controls and 500+ third parties using pre-built analytics to create multi-vector, multi-vendor detections and AI-powered automation to reduce incident response times. The complete GenAI-powered Trellix Security Platform delivers the advanced security controls required to improve cyber hygiene across endpoints, servers, networks, data, cloud, and mobile devices. Built on over a decade of AI modeling and 25 years in analytics and machine learning, Trellix Wise GenAI capabilities relieve alert fatigue and surface stealthy threats. Trellix Consulting Services can assess your current security program against international and European standards, providing readiness assessments and threat intelligence for continuous risk analysis.

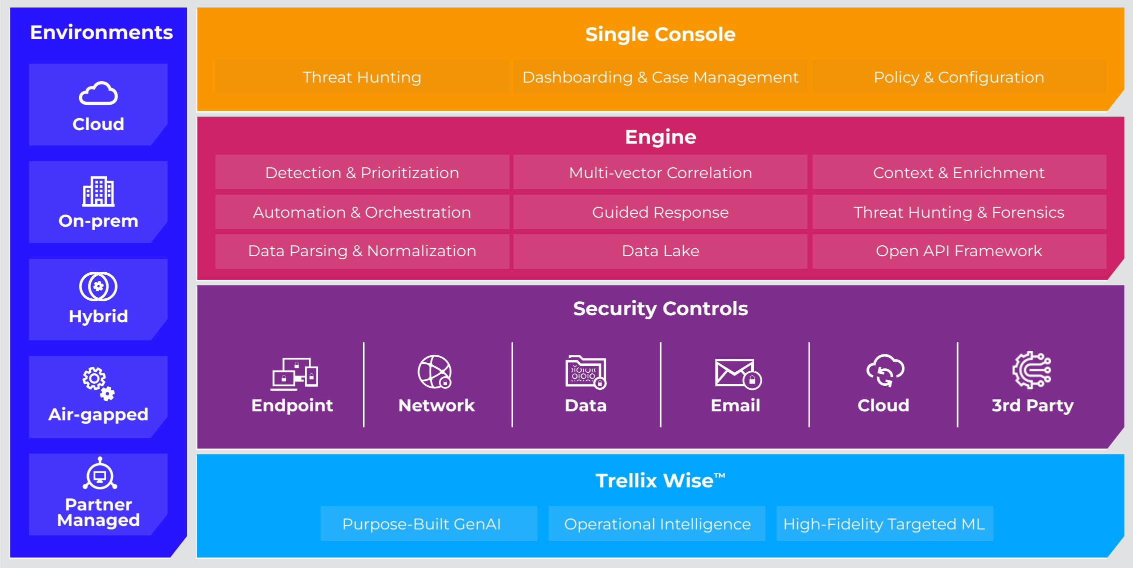

Figure 1: Trellix Security Platform

Specific compliance requirements may vary depending on member state implementation guidance, but the common thread for NIS-2 compliance is cyber risk reduction and resilience. Below we outline the top five ways where Trellix, in collaboration with our partner solutions, can help you meet NIS-2 requirements and manage your risk of emerging threats.

Identify your risk with Trellix assessment services

The NIS-2 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. The compliance timeline is fast approaching. It is important to assess your current state against one of those standards and your readiness in potential high-risk areas. Based on our experience and Trellix threat intelligence, we recommend focusing on these 5 key assessments.

Trellix Solutions	Solution Description	Related NIS-2 Articles
Cyber Security 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, XDR 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

You can schedule Trellix Assessment Services through your Account Manager or on the website here.

Build your ransomware resilience

Our recent Trellix CyberThreat Report describes the escalation in ransomware attacks as new threats make an increasingly notable impact. Ransomware is a significant threat to the entities delivering essential services governed by NIS-2. High-profile attacks have affected energy, transportation, and public administration, 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 NIS-2 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 IVX for Collaboration Applications	Prevent and detect ransomware delivery from phishing 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 Connect	Unite signals from multiple tools to surface ransomware threats that might go undetected by individual point tools.	21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j

To learn more about how Trellix can protect your business from ransomware, please visit our Ransomware Detection and Response website here.

Accelerate SecOps threat detection and response

One of the main goals of the NIS-2 Directive is to improve incident detection and response across the enterprise. Many operators of essential services likely face common Security Operation Centre (SOC) challenges such as visibility gaps, talent shortage, and lack of automation. Our SOC and incident response (IR) assessments expose those gaps and help you design an action plan to remediate and mature the program. From a technology perspective, Trellix Helix Connect reduces analyst workload and mean time to respond (MTTR) with an open security platform that integrates data from Trellix sensors and 500+ integrations. 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 Connect and SOC assessments, we recommend the following Trellix solutions to provide deep visibility and threat detection across the enterprise.

Trellix Solutions	Solution Description	Related NIS-2 Articles
Trellix EDR and Trellix Endpoint Forensics	Provides deep endpoint visibility, malicious activity detection, and IR forensics	21.2b, 21.2g
Trellix NDR and Trellix 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 Connect	Delivers XDR capability 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
Semperis (Partner)	Protects Directory Services and integrates with Helix Connect for identity detection and response capabilities	21.2g, 21.2i

Protect your operational technology networks and systems

Many entities delivering essential services governed by NIS-2 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 GenAI-powered Trellix Security Platform 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 behaviour. In addition to Trellix Endpoint Security, 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 NIS-2 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)**	Discover SCADA asset details and vulnerabilities, integrate with XDR for threat detection and response	21.2e, 21.2b
Trellix Helix Connect	Correlates data from multiple sources including OT and IoT devices to create the full picture of a threat	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 risk of a data breach incident

Protection of 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 a risk of compromise from external and internal threats. In fact, according to the 2024 Verizon Data Breach Investigations Report, 68% of breaches were caused by insider risk. External APT actors are leveraging AI to generate exploits faster and this puts your sensitive customer and corporate data at risk of exposure through vulnerable applications. As NIS-2 dictates short reporting timelines for a data breach incident, it's time 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 Data Loss Prevention Discover will scan your network and repositories like SharePoint improving the visibility and classification. Those will help get you started but for full protection we recommend implementing the following Trellix Data Security controls to mitigate risk of a data breach from device to cloud.

Trellix Solutions	Solution Description	Related NIS-2 Articles
Trellix Endpoint Data Protection and Discovery	Discover, classify, and protect data on the endpoint	21.2h, 21.2i
Trellix Network Data Protection and Discovery	Discover, classify, and protect data across the network	21.2i
Trellix Database Security	Monitor and control access to sensitive information in application databases	21.2i
Trellix Helix Connect	Delivers XDR capability to improve data detect and respond	21.2d, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j
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 NIS-2, please register for our webinar "Achieving NIS-2 Compliance with Trellix" or schedule a workshop with your Trellix representatives.