SOPHOS

The NIS 2 Directive

The EU Network and Information Security (NIS) directive was the first piece of EU-wide legislation on cybersecurity that came into force in 2016. However, to address the limitations identified within the current framework and to respond to the growing cybersecurity threats in the EU in the wake of digitalization and Covid-19, the European Commission has replaced the NIS Directive with the NIS 2 Directive that introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonizing sanctions regimes across Member States. The NIS 2 Directive entered into force on January 16, 2023, and the Member States have 21 months, until October 17, 2024, to transpose the directive into national law.

The NIS 2 Directive aims to strengthen security requirements in the EU by expanding its scope to more sectors and entities; taking into account measures like risk analysis and information system security policies, incident handling, and supply chain security; and streamlining reporting obligations, among others. In case of non-compliance, NIS 2 requires member states to provide hefty penalties: €10 million or 2% of global turnover (whichever is higher) for essential entities and €7 million or 1.4% of global turnover (whichever is higher) for important entities. NIS 2 imposes direct obligations on the management bodies to implement and supervise their organization's compliance with the legislation. Non-compliance could potentially lead to the imposition of a temporary ban from discharging managerial responsibilities on the senior management of the entity, including the C-Suite level executives.

This document outlines how Sophos solutions offer effective tools to support organizations in addressing Chapter IV of the NIS 2 Directive, Cybersecurity Risk-Management Measures and Reporting Obligations, and eventually help them comply with the NIS 2 Directive.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. The use of Sophos products alone does not guarantee legal compliance. The information in this document does not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations and should consult their own legal counsel for advice regarding such compliance.

NIS 2 Directive - Chapter IV, Cybersecurity Risk-Management Measures and Reporting Obligations

NIS 2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
Chapter IV, Article 20, Governance		
2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, to data loss prevention, password protection and more.
	Sophos Training and Certifications	Training courses and certifications to help partners and customers get the best out of Sophos security deployments, access to latest know-how and expertise for security best practices.
Chapter IV, Article 21, Cybersecurity risk-management measures		
2. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems… based on a) policies on risk analysis and information system security;	Sophos Endpoint	Delivers unmatched protection against ransomware and breaches. Innovative protection capabilities, including AI-powered deep learning, anti-exploitation, airtight ransomware protection with automatic rollback, and adaptive defenses that automatically respond to adversaries and stop even the most advanced attacks.
	Sophos Firewall	Delivers industry-leading network protection optimized for the modern encrypted internet and distributed user base. Comprehensive SD-WAN capabilities securely connect distributed offices and locations while built-in ZTNA delivers secure user-based access from any location. Sophos Firewall integrates with Sophos Endpoint, Sophos ZTNA, Sophos Switches, and Wireless Access Points, as well as Sophos XDR and Sophos MDR to automatically respond to threats, stopping attacks before they can spread. Compromised hosts are automatically isolated, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
	Sophos Managed Detection and Response (MDR)	Continuously monitors signals from across the security environment, including network, email, firewall, identity, endpoint, and cloud technologies, to quickly and accurately detect and respond to potential cybersecurity events. Proactive threat hunting identifies threats before they can impact the organization.

NIS 2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with Sophos-managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
	Sophos Cloud Optix	Enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. It continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
2. b) incident handling;	Sophos Endpoint	Automatically detects and blocks 99.98% of attacks. Provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
	Sophos Firewall	Its extensive on-box and cloud-based logging and reporting tools provide actionable insights to guide and accelerate incident response, including deep intelligence into network activity and easy log access for forensic analysis. Automated threat response (in collaboration with other Sophos products) reduces response time from minutes to seconds, stopping attacks before they can spread.
	Sophos Managed Detection and Response (MDR) Complete	Includes unlimited full-scale incident response as standard, providing 24/7 coverage delivered by incident response experts. Includes full root cause analysis and reporting. Our average time to detect, investigate and respond is just 38 minutes.
	Sophos Network Detection and Response (NDR)	When Sophos NDR identifies an indicator of compromise, active threat, or adversary, analysts are immediately alerted and can instantly push a threat feed to Sophos Firewall to trigger an automated response to isolate the compromised host.

NIS 2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
	Sophos XDR	Enables analysts to detect, investigate, and respond to incidents across key attack surfaces using an organization's existing security solutions (Sophos and non-Sophos). Sophos XDR stores 90 days' security telemetry in the Sophos data lake to facilitate incident handling, while optimized workflows and AI-powered capabilities accelerate incident investigation and response.
	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
2. c) business continuity, such as backup management and disaster recovery, and crisis management;	Sophos Endpoint	Uses innovative and adaptive security technologies to prevent business disruption, including AI-powered deep learning, anti-exploitation, and airtight ransomware protection with automatic rollback.
	Sophos Firewall	Sophos Firewall's plug-and-play high availability (HA) clusters deliver resiliency in the face of business interruption. For improved cost efficiency, customers get active/passive redundancy while only needing to purchase a license for the active device. Sophos Firewall also supports multiple internet links with zero impact fail-over and load balancing across wireless LTE, cable, DSL, and fiber for maximum resiliency. Extensive logging and on-box and cloud-based reporting provides deep, actionable telemetry to facilitate disaster recovery.
	Sophos Managed Detection and Response (MDR)	Mitigates the risk of business disruption with 24/7 detection and response. In the event of an incident, it includes a full incident response service. Integrations with backup and recovery vendors enable analysts to identify when adversaries are targeting backups so they can quickly step in and neutralize the attack. The service stores up to a year's security telemetry in the Sophos data lake, facilitating disaster recovery.
	Sophos XDR	Stores 90 days' security telemetry in the Sophos data lake, facilitating disaster recovery. Integrations with backup and recovery vendors enable analysts to identify when adversaries are targeting backups so they can quickly step in and neutralize the attack.

NIS 2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
	Sophos Cloud Optix	Identifies where backups are not being taken within public cloud infrastructure accounts and alerts the security team within the Cloud Optix console to take action.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
2. d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Sophos Endpoint	Delivers comprehensive defense in depth against threats that get in via third-party suppliers. Protection capabilities include AI-powered deep learning, anti-exploitation, airtight ransomware protection with automatic rollback, and adaptive defenses that automatically respond to adversary behaviors.
	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf. Extensive integrations with security and business solutions used across the organization (including Microsoft and Google) enable us to see and mitigate threats via your technology supply chain.
	Sophos XDR	Enables analysts to detect, investigate and respond to suspicious activity across their environment, helping them see and stop supply chain attacks. Sophos NDR (an add-on to Sophos XDR) sits deep within the network, monitoring ALL network traffic to identify threats that other solutions may miss – including from supply chain partners.
	Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.
2. e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Sophos Firewall	Sophos Firewall is 'Secure by Design,' and we continually work to make it the most difficult firewall for adversaries to compromise. It includes: › Best practices built-in to optimize customer security › Hardening against attacks with secure remote management, containerization, strict access management, MFA and more › Automated hot-fix response with over-the-air-updates to address urgent security issues › Proactive monitoring of the global firewall install base › Robust and transparent vulnerability disclose program, with market-leading bug bounties

NIS 2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
	Sophos Managed Detection and Response (MDR)	Sophos MDR's expert analysts monitor alerts from across the network 24/7, investigating suspicious activities and neutralizing attacks. Sophos NDR sits deep within the network, monitoring ALL network traffic to identify threats that other solutions may miss. Sophos MDR proactively responds to vulnerability disclosure by the client. On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. A full human-authored report is provided in response to the disclosure investigation. Sophos Managed Risk is a fully-managed vulnerability management service that identifies exposures and provides risk-based patching guidance. It collaborates with and complements the Sophos MDR service. Sophos is committed to 'Secure by Design.' We have a robust and transparent vulnerability disclosure program, including safe harbor provisions to support researchers and market-leading bug bounties.
	Sophos XDR	Enables analysts to monitor alerts from across the network 24/7, investigating suspicious activities and neutralizing attacks. Sophos NDR (an add-on to Sophos XDR) sits deep within the network, monitoring ALL network traffic to identify threats other solutions may miss.
	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
	Sophos Rapid Response Service	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

NIS 2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
2. f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	Sophos Endpoint	Built-in health check enables organizations to quickly identify and address configuration issues with their Sophos-protected devices. Should an issue be identified, the 'Fix Automatically' option enables users to address insecure configurations in just a few clicks.
	Sophos Firewall	Built-in posture reports enable organizations to quickly assess their network security deployment and identify areas for optimization.
	Sophos Managed Detection and Response (MDR)	Investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk levels and prioritize response.
2. g) basic cyber hygiene practices and cybersecurity training;	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics , from phishing and cybersecurity overview lessons to data loss prevention, password protection, and more.
	Sophos Training and Certifications	Training courses and certifications to help partners and customers get the best out of Sophos security deployments, access to latest know-how and expertise for security best practices.
2. h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Sophos Firewall	Facilitates MFA for VPN connections, with granular RADIUS/TACACS integration. The Sophos Cryptographic Module incorporated into the Sophos Firewall systems provides FIPS 140-2 validated cryptography for the protection of sensitive information.
	Sophos Email	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.

NIS 2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
2. i) human resources security, access control policies and asset management;	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, giving user-level controls over applications, bandwidth, and other network resources. Built-in ZTNA delivers secure user-based access from any location. Role-based admin controls, multi-factor authentication, and granular access controls are also included.
	Sophos Managed Detection and Response (MDR)	Threat-hunting experts monitor and correlate information system activity across the full IT security environment, identifying and investigating suspicious activities by regularly reviewing records of information system activity, including relating to HR system, access control and assets.
	Sophos XDR	Enables analysts to monitor and correlate information system activity across the full security environment, identifying and investigating suspicious activities, including those relating to HR systems, access control and assets.
	Sophos Central	Keeps access lists and user privileges information up to date. Procedures are in place to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
	Sophos Cloud Optix	Facilitates inventory management across multiple-cloud providers with continuous asset monitoring and complete network topology and traffic visualization.
	Sophos ZTNA	Enables better security and more agility in quickly changing environments by making it quick and easy to enroll or decommission users and devices. Continuously validates user identity, device health, and compliance before granting access to applications and data.
2. j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	Sophos Firewall	Supports flexible MFA authentication options including role-based admin controls, and directory services for access to key system areas. Built-in ZTNA continuously validates user identity, device health, and compliance before granting access to applications and data. Granular access controls are also integrated into Sophos Firewall to govern access.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
	Sophos Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.

NIS 2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
Chapter IV, Article 23, Reporting obligations		
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: d) a final report not later than one month after the submission of the incident notification under point (b), including the following: (i) a detailed description of the incident, including its severity and impact;	Sophos Managed Detection and Response (MDR)	Includes full incident response and root cause analysis. Sophos experts remediate the incident and provide a full human-authored report that includes detailed analysis of how the attack occurred together with guidance on how to harden the environment against future exploitation.
	Sophos XDR	Enables analysts to identify and report on the full attack chain, including a detailed description of the incident and the root cause of the attack.
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: d) a final report not later than one month after the submission of the incident notification under point (b), including the following: (ii) the type of threat or root cause that is likely to have triggered the incident;	Sophos Managed Detection and Response (MDR)	Includes full incident response and root cause analysis. Sophos experts remediate the incident and provide a full human-authored report that includes detailed analysis of how the attack occurred together with guidance on how to harden the environment against future exploitation.
	Sophos XDR	Enables analysts to identify and report on the full attack chain, including a detailed description of the incident and the root cause of the attack.

2024-08-26 (WP-NP)

SOPHOS