NIS Directive Cyber Assessment Framework

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. The NIS Directive applies primarily to Operators of Essentials Services (OES) that are identified by EU Member States and Digital Services Providers (DSP) that offer key digital services to persons within the EU. The NIS Directive entered into force in August 2016. EU member states – including the UK –were required to transpose the NIS Directive into their national laws by 9 May, 2018.

In the UK, the NIS Directive requires OESs to perform a self-assessment of their security posture using the Cyber Assessment Framework (CAF). Developed by the NCSC (National Cyber Security Centre), the CAF offers guidance to organizations to assess themselves against 14 security principles and summarizes the acceptable security levels for organizations under the Regulations' requirements. This document maps out how Sophos solutions offer effective tools to support organizations in addressing the NIS Cyber Assessment Framework and eventually help them to comply with the NIS 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.

Security principle	Guidance	Sophos solution	How it helps
Objective A: Managing security risk			
A1 Governance	Appropriate organizational structures, policies, and processes in place to understand, assess, and systematically manage security risks to the network and information systems supporting essential services.		
A1.b Roles and responsibilities	Your organization has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	All Sophos products	Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
		Sophos Firewall	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization.
		Sophos Central	Configurable role-based administration provides granular control of administrator privileges.

Security principle	Guidance	Sophos solution	How it helps
A2 Risk Management	The organization takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organizational approach to risk management.		
A2.a **Risk Management Process**	Your organization has effective internal processes for managing risks to the security of network and information systems related to the delivery of essential services and communicating associated activities	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also helps to identify and protect users and applications on the network. Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network.
		Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
		Sophos Cloud Optix	Establishes guardrails to prevent, detect, and remediate accidental or malicious changes in network configuration, network traffic, resource configuration, and user behavior or activities.
		Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos Managed Detection and Response (MDR)	Threat-hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high-caliber, actional signals across the network infrastructure to optimize cyber defenses.
A3 Asset Management	Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people, and systems, as well as any supporting infrastructure (such as power or cooling).		
A3.a **Asset Management**	Asset Management	Sophos Cloud Optix	Inventory management across multiple-cloud providers with continuous asset monitoring and complete network topology and traffic visualization.
A4 Supply Chain	The organization understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third-party services are used. Regardless of your outsourcing model the OES remains responsible for the security of the service and, therefore, all the requirements that come from the NIS Directive.		
A4.a **Supply Chain**	Supply Chain	Sophos Intercept X with XDR	Provides comprehensive defense in depth against threats that get in via third-party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
		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.
		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.

Security principle	Guidance	Sophos solution	How it helps
Objective B - Protecting against cyber-attack			
B1 Service Protection Policies and Processes	The organization defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services		
B1.a Policy and Process Development	You have developed and continue to improve a set of service protection policies and processes that manage and mitigate the risk of cybersecurity-related disruption to the essential service.	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
		Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
		Sophos Cloud Optix	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.
		Sophos Email Sophos Firewall	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
		Sophos Managed Detection and Response (MDR)	Sophos MDR swiftly contains and neutralizes incidents, with average time to detect, investigate and respond to just 38 minutes. Clients choose the level of response they wish us to take.
B2 Identity and Access Control	The organization understands, documents, and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated, and authorized.		
B2.a Identity Verification, Authentication and Authorization	You robustly verify, authenticate and authorize access to the networks and information systems supporting your essential service.	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. Supports flexible multi-factor authentication options including directory services for access to key system areas.
		Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
		Sophos Cloud Optix	Sophos Cloud Optix, Cloud Security Posture Management solution, connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		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).

Security principle	Guidance	Sophos solution	How it helps
B2.b Device Management	You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential service.	Sophos Intercept X Sophos Intercept X for Server	Enforces web, data, and device policies to allow only authorized applications to be run, devices to be connected and data to be distributed.
		Sophos Wireless	Monitors the health status of any Sophos-managed endpoint or mobile device and automatically restricts web access on trusted Wi-Fi networks for those with serious compliance issues.
		Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
		Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
B2.c Privileged User Management	You closely manage privileged user access to networks and information systems supporting the essential service.	Sophos Cloud Optix	Includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Configurable role-based administration provides granular control of administrator privileges. Keeps access lists and user privileges information up to date. Provides procedures 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 Wireless	Provides controlled internet access and hotspots for visitors, contractors, and other guests on the network using enterprise-grade backend authentication for a seamless user experience.
B2.d Identity and Access Management (IdAM)	You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential service.	All Sophos products	Sophos' user-identity-based technology powers all policies and reporting across all Sophos products. This allows organizations to enforce role-based user-level controls over network resources and other organizational assets and trace the actions of individual users.
		Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, enabling user-level access controls.
		Sophos Central	Keeps access lists and user privileges information up to date. Provides procedures 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).
B3 Data Security	Data stored or transmitted electronically is protected from actions such as unauthorized access, modification, or deletion that may cause disruption to essential services. Such protection extends to how authorized users, devices and systems access critical data necessary for the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.		
B3.b Data in Transit	You have protected the transit of data important to the delivery of the essential service. This includes the transfer of data to third parties.	Sophos Email	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.

Security principle	Guidance	Sophos solution	How it helps
B3.c Stored Data	You have protected stored data important to the delivery of the essential service.	Sophos Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and can prevent leaks of such information via email, uploads, and local copying.
		Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
		Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
		Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest. Monitors AWS, Azure and GCP accounts for cloud storage services without backup schedules enabled and provides guided remediation.
		Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
B3.d Mobile Data	You have protected data important to the delivery of the essential service on mobile devices.	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
B4 System Security	Network and information systems and technology critical for the delivery of essential services are protected from cyber-attack. An organizational understanding of risk to essential services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.		
B4.a Secure by Design	You design security into the network and information systems that supports the delivery of essential services. You minimise their attack surface and ensure that the delivery of the essential service should not be impacted by the exploitation of any single vulnerability.	Sophos Firewall	Flexible and powerful segmentation options via zones and VLANs provide ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network. Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
		Sophos Switch	Allows configuration of VLANs to segment your internal traffic and reduce the attack surface in case of an infection or breach. Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
		Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
		Synchronized Security in Sophos products	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised/unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.

Security principle	Guidance	Sophos solution	How it helps
		Sophos Cloud Optix	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. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Managed Detection and Response (MDR)	24/7 detection, investigation and neutralization of suspicious activities by human experts enables us to identify and stop exploitation of vulnerabilities by adversaries. Sophos X-Ops experts keep operators up-to-date on the latest threat and vulnerability developments.
B4.b Secure Configuration	You securely configure the network and information systems that support the delivery of essential services.	Sophos Cloud Optix	Sophos's cloud security posture management solution, Sophos Cloud Optix, enables teams to proactively improve security posture, detecting insecure configurations and vulnerabilities. By automatically mapping security and compliance standards to your environments, Cloud Optix provides the visibility needed to monitor and maintain security posture 24/7.
		Sophos Firewall	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports, and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. Provides complete application visibility and control over all applications on your network with deep-packet scanning technology and Synchronized App Control that can identify all the applications that are currently going unidentified on your network. Sophos' Web Protection engine is backed by SophosLabs and includes advanced web protection, Potentially unwanted App control, and more, to identify and block the latest web threats and unwanted apps.
		Sophos Intercept X Sophos Intercept X for Server	Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications. Sophos Intercept X for Server does not permit unauthorized applications from running, automatically scanning your system for known good applications, and whitelisting only those applications.
		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.
		Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event
B4.c Secure Management	You manage your organization's network and information systems that support the delivery of essential services to enable and maintain security.	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
		Sophos Cloud Optix	Proactively identifies an unsanctioned activity, vulnerabilities, and misconfigurations across AWS, Azure, and GCP. Complete cloud edge firewall solution includes IPS, ATP, and URL filtering and lets you deploy several network security products at once to protect your hybrid cloud environments against network threats..
		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.
		Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.

Security principle	Guidance	Sophos solution	How it helps
		Sophos XDR	Detects and investigates across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.
B4.d. Vulnerability Management	You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.	Sophos Firewall	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications/software packages; Synchronized Application Control in Sophos Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications Deny access to email, network, and other resources if device is not in compliance with policy.
		Synchronized Security in Sophos products	Sophos Firewall's Synchronized Security Endpoint Integration identifies all unknown, evasive, and custom applications running on your network so you can easily identify rogue applications like Psiphon and block them.
		Sophos Cloud Optix	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 Managed Detection and Response (MDR)	Sophos 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 level and prioritize response.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Endpoint Protection application control policies restrict the use of unauthorized applications.
B5 Resilient Networks and Systems	The organization builds resilience against cyber-attack and system failure into the design, implementation, operation, and management of systems that support the delivery of essential services.		
B5.c Backups	You hold accessible and secured current backups of data and information needed to recover.	Sophos Cloud Optix	Monitors AWS, Azure and GCP accounts for cloud storage services without backup schedules enabled and provides guided remediation.
B6 Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organizational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.		
B6.b Cyber Security Training	The people who operate and support your essential service are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.	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.
		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, through to data loss prevention, password protection and more.

Security principle	Guidance	Sophos solution	How it helps
Objective C - Detecting cyber security events			
C1 Security Monitoring	The organization monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.		
C1.a Monitoring Coverage	The data sources that you include in your monitoring allow for the timely identification of security events which might affect the delivery of your essential service.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		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 Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
		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.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
C1.b Securing Logs	Logging data should be held securely and read access to it should be granted only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.	Sophos Firewall	Stored logs cannot be accessed, destroyed, or altered without administrator privileges. To prevent accidental destruction due to destruction of firewall device altogether, the logs can be integrated into independent syslog server or into Sophos Central.
C1.c Generating Alerts	Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts	Sophos Firewall	Stored logs cannot be accessed, destroyed, or altered without administrator privileges. To prevent accidental destruction due to destruction of firewall device altogether, the logs can be integrated into independent syslog server or into Sophos Central.
		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 Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
		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.

Security principle	Guidance	Sophos solution	How it helps
C1.d Identifying Security Incidents	You contextualize alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		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 Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
		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.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
C1.e Monitoring Tools and Skills	Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats, and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential services they need to protect.	Sophos Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
C2 Proactive Security Event Discovery	The organization detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services, even when the activity evades standard signature-based security prevent/detect solutions, or when it is not possible to use signature-based detection, for some reason.		
C2.a System Abnormalities for Attack Detection	You define examples of abnormalities in system behavior that provide practical ways of detecting malicious activity that is otherwise hard to identify.	Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Intercept X consistently looks at reported false positives and false negatives to ensure the product is being continuously improved. It integrates a deep learning malware detection model that can scale to hundreds of millions of training samples and can 'memorize' the entire observable threat landscape as part of its training process. It is regularly trained by our SophosLabs team to stay up to date over time.
		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 XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.

Security principle	Guidance	Sophos solution	How it helps
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates suspicious signals, correlating data and behaviors and leveraging Sophos X-Ops threat intelligence for context and insights. On notification of vulnerabilities, Sophos MDR proactively hunts for exposure to enable swift remediation. Once an incident is remediated, Sophos MDR performs full root cause analysis which enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
C2.b Proactive Attack Discovery	You use an informed understanding of more sophisticated attack methods and of normal system behavior to monitor proactively for malicious activity.	Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates suspicious signals, correlating data and behaviors and leveraging Sophos X-Ops threat intelligence for context and insights. On notification of vulnerabilities, Sophos MDR proactively hunts for exposure to enable swift remediation.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
Objective D- Minimizing the impact of cyber security incidents			
D1 Response and Recovery Planning	There are well-defined and tested incident management processes in place, that aims to ensure the continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.		
D1.b Response and Recovery Capability	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.	Sophos Managed Detection and Response (MDR)	Sophos 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 level and prioritize response.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
D2 Lessons Learned	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.		
D2.a Incident Root Cause Analysis	Your organization identifies the root causes of incidents you experience, wherever possible.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Managed Detection and Response (MDR)	Threat-hunting organization experts monitor and correlate information system activity across the full IT security environment, identifying and investigating suspicious activities.
		Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Intercept X Sophos Intercept X for Server	Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be.

Security principle	Guidance	Sophos solution	How it helps
D2.b Using Incidents to Drive Improvements	Your organization uses lessons learned from incidents to improve your security measures.	Sophos Intercept X Sophos Intercept X for Server	Intercept X consistently looks at reported false positives and false negatives to ensure the product is being continuously improved. It integrates a deep learning malware detection model that can scale to hundreds of millions of training samples and can 'memorize' the entire observable threat landscape as part of its training process. It is regularly trained by our SophosLabs team to stay up to date over time.
		Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a 24/7 team of response experts. Once an incident is remediated, Sophos MDR performs full root cause analysis which enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.
		SophosLabs	Delivers the global threat intelligence advantage with Sophos' state-of-the-art big data analytics system that efficiently processes millions of emails, URLs, files, and other data points analyzed each day. This data, along with our extensive experience, enables us to develop new definitions, detect entire classes of threats, and even new variants. And, Live Protection and Live Anti-spam offer the data and expert analysis from SophosLabs in real time.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com