Reference Card for Education

The education sector remains a prime target for cybercriminals because of its sheer size and the large attack surface that offers the potential for significant financial gains. Sophos secures educational institutions against a wide range of cyberattacks, including human-led threats that technology alone cannot prevent. From managed detection and response (MDR) to endpoint and network security, Sophos enables organizations to optimize their defenses and frees IT teams to focus on the business.

This document provides a general reference showing how Sophos solutions assist organizations in the education sector in meeting their cybersecurity requirements.

CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing against human-led attacks, including ransomware	Sophos Managed Detection and Response (MDR)	A fully managed, 24/7 service delivered by experts specializing in detecting and responding to cyberattacks stops advanced human-led attacks on your behalf, neutralizing threats before they can disrupt business operations or compromise sensitive customer data.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	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 like ransomware 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.
Identity and access management	All Sophos products	Sophos' user-identity-based technology allows user-level controls over network resources and other organizational assets.
	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, enabling user-level control over applications, bandwidth and other network resources. Supports flexible multi-factor authentication options including directory services for access to key system areas.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Cloud Optix	The SaaS based service 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. 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.

CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing the network	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. Supports flexible multi-factor authentication options including directory services for access to key system areas. 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.
	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	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.
	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.
Securing remote access of users	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 neutralize the event quickly.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data. It authenticates requests for access from trusted users, irrespective of the location.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	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 Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Controls remote access authentication and user monitoring for remote access and logs all access attempts.
BYOD Management	Sophos Mobile	Supports BYOD environments through the Android Enterprise Work Profile and iOS User Enrolment modes of management. Corporate emails and apps can be deployed to a device while these remain separate from a user's personal data. Admins retain control over corporate content without intruding on the users' privacy.
Protection from harmful/ unproductive content	Sophos Firewall	Provides logging, monitoring, and even enforcement of policies related to keyword lists on bullying, radicalization, or self-harm (for example). You can schedule reports to identify users at risk and get details about their activities, including what and where they are posting or what sites they are visiting. Built-in policies for pre-defined activities like "Not Suitable for Schools" as well as features like SafeSearch, and YouTube restrictions enable child safety online. 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.

CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing research and personal data of students and staff	Sophos Intercept X	Stops the latest cybersecurity threats to users' endpoint devices, such as ransomware, file-less attacks, exploits, and malware, even when they have never been seen before. DLP capabilities detect sensitive data and prevent leaks of such information via email, uploads, and local copying.
	Synchronized Security feature 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.
	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 Central Device Encryption	Enables protection of devices and data with full disk encryption for Windows and macOS to help you keep research and user data secure.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data. The integration of Sophos Endpoint and Sophos ZTNA allows them to share status and health information to automatically prevent compromised hosts from connecting to networked resources, preventing threats from moving laterally and getting a foothold on your network.
	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	Cloud Optix continually monitors public cloud infrastructure to provide visibility of resources and threats across your organization and proactively reduce business risk from unsanctioned activity, vulnerabilities, and misconfigurations that would leave internal records exposed.
	Sophos Email	AI-powered smart email security delivers robust protection against email borne threats – emails from malicious URLs / C2 servers, spams, ransomware and phishing campaigns etc. Blends multiple authentication techniques, AI, threat intelligence and blocking features to deliver pervasive email security. Also provides advanced data breach prevention with policy-based email encryption to protect sensitive data.
Ensuring child safety and compliance	Sophos Firewall	Allows built-in features and policy settings that help you become compliant with local regulations easily. Built-in policies for pre-defined activities like "Not Suitable for Schools" as well as features like SafeSearch, YouTube restrictions, and keyword filtering (related to bullying, radicalization, or self-harm (for example)) enable child safety online.
Protection from phishing scams	Sophos Email	Scans all inbound messages for key phishing indicators such as brand spoofing and impersonation attempts in real-time using SPF, DKIM, and DMARC authentication techniques and email header anomaly analysis. This helps to spot and block phishing emails before they reach your users. Multi-rule DLP policies for groups and individual users ensure the protection of sensitive information with discovery of financials, confidential contents, and PII in all emails and attachments.
	Sophos Intercept X	Offers complete protection for all endpoints – Windows, Mac, Linux, and virtual machines – with layered protection against advanced attacks.
	Sophos Phish Threat	Offers a collection of more than 30 security awareness training modules to educate and test your end users through automated attack simulations, quality security awareness training, and actionable reporting metrics.

CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Protection against unsafe and unproductive apps	Sophos Firewall	Get customizable policies for granular control over thousands of apps on your network with Sophos Firewall's superior application visibility and controls. Prevent students from accessing unproductive apps with Sophos Firewall's Synchronized Security integration with endpoint protection that identifies all unknown, evasive, and custom applications running on your network so you can easily identify rogue applications like Psiphon and block them. With CASB cloud app visibility, identify all the browser apps and cloud services that are in use on your network to identify and control shadow IT and data at risk.
	Sophos Intercept X Sophos Intercept X for Server	Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. 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.
	Sophos Cloud Optix	Continually monitors public cloud infrastructure to provide visibility of resources and threats across your organization and proactively reduce business risk from unsanctioned activity, vulnerabilities, and misconfigurations that would leave internal records exposed.
	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.
Managing risky users	Sophos Firewall	Correlates each user's surfing habits and activity with advanced threat triggers and history to identify users with risky online behavior. You can schedule reports to identify users at risk and get details about their activities, including what and where they are posting or what sites they are visiting. Automatically isolates compromised systems to stop active attacks in their tracks , denying further intrusion into the school network. Offers the most extensive set of user authentication options available on any firewall, including Active Directory integration, Chromebook support, and even our unique and easy-to-use Synchronized User ID solution that facilitates seamless user authentication across the firewall and endpoints to offer tighter, granular user access, blocking an external attacker as well as a malicious insider from gaining access to sensitive systems or data.
Identifying, resolving and investigating security incidents	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 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 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. Includes rollback to original files after a ransomware or master boot record attack. Provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.

CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Managing compliance with regulatory requirements or security best practices	Sophos Cloud Optix	Continuously monitor compliance with custom or out-of-the box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2. Automatically analyze cloud configuration settings against compliance and security best practice standards without diverting resources. Prevent compliance gaps leaving you exposed with a single view of compliance posture across AWS, Azure, and Google Cloud.
	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 neutralize the event quickly.

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

Oxford, UK

2023-03-28 RC-NA (PS)