Reference Card for Education

The IT infrastructure of schools and colleges is often protected by traditional security systems that are unable to address cybersecurity challenges like phishing or advanced malware attacks like ransomware. These institutions also find it difficult to comply with regulations such as the Children's Internet Protection Act (CIPA) and the General Data Protection Regulation (GDPR).

Sophos offers next-gen security solutions to higher education, K-12, and primary or secondary education institutions to enable them to protect against the increasingly sophisticated cyberattacks and also manage trends such as BYOD and more.

This document provides a general reference showing how Sophos products assist organizations in the education sector to meet their cybersecurity requirements.

Challenge	Sophos Product	How it helps
Exposure to 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 CIPA and 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.
Unauthorized Disclosure of Student and/or Educator Data	Sophos SD-WAN/ Sophos Firewall	Securely connect sites across your geographically distributed network and securely exchange personal student and staff information and financial transactions.
	Sophos Firewall	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 Central Device Encryption	Enables protection of devices and data with full disk encryption for Windows and macOS to help you keep personal student and educator data secure.
	Sophos Zero Trust Network Access (ZTNA)	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption helps to keep sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection enables safeguarding your users and devices from malicious content and apps.

SOPHOS

Challenge	Sophos Product	How it helps
	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.
Web Filtering Policies for Student 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 CIPA and 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.
Phishing Protection	Sophos Email	Pre-Delivery: Email authentication uses a combination of authentication techniques (SPF, DKIM, DMARC) to enable only legitimate emails from trusted sources to enter your inbox.
	Sophos Intercept X	Post-Delivery: If students/educators click on a malicious link, root cause analysis tells you which files, processes, and registry keys were hit by malware; Synchronized Security automatically isolates infected endpoints and instantly cleans up malware.
	Sophos Phish Threat	Educates and tests end users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics.
BYOD Management	Sophos Mobile	Manage, secure, configure, and set up traditional and mobile endpoints and ensure uniform security policies regardless of device type or ownership. Container-only management allows email and data to be protected and controlled without intruding on user privacy.
Unauthorized Data Upload, Unproductive Cloud Apps Access	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 Endpoint Integration 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	Endpoint Protection application control policies restrict the use of unauthorized applications. Device Control allows admins to control the use of removable media through policy settings.
	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 Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption helps to keep sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection enables safeguarding your users and devices from malicious content and apps.
	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 Zero Trust Network Access (ZTNA)	Continuously validates user identity, device health, and compliance before granting access to applications and data.
Ransomware Protection	Sophos Intercept X	Enables ransomware file protection, automatic file recovery, and behavioral analysis to stop ransomware and boot record attacks.

Challenge	Sophos Product	How it helps
Advanced malware and threats	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.
	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. Lateral Movement Protection, a Synchronized Security feature, prevents the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
	Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Managed Threat Response (MTR)	Proactive 24/7 threat hunting by elite team of threat analysts initiates actions to remotely disrupt, contain, and neutralize threats on your behalf to stop even the most sophisticated threats. Incorporates vulnerability intelligence to provide educational institutions with proactive security posture improvements.
	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 Wireless	Offers visibility into wireless networks health and clients [visitors, staff, and students] connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
	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 enable pervasive email security. Also provides advanced data breach prevention with policy-based email encryption to protect sensitive data.
	Sophos Intercept X for Mobile	Enables detection of 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.
Manage Risky Users (Insider Threats)	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.
Identity and Access Management	Sophos Firewall	Get next-gen granular control over the applications in use, your users' web surfing, bandwidth allocation, and other network resources with the help of our user identity-based firewall policies and reporting.
	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. And 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.

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

© Copyright 2021. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2021-10-19 RC (PC)

SOPHOS