SOPHOS

Cybersecurity Guide for the Education Sector

Sophos' expert threat analysts and world-leading threat intelligence help you to identify and respond to advanced threats faster, 24/7.

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. The number of devices and diversity of operating systems in the network, the increased use of e-learning tools leading to new vulnerabilities, and the varying degrees of technical knowledge in students, teachers, and administrative staff that loosen up cybersecurity in favor of usability are all the factors that affect this industry which is usually understaffed and underfunded.

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.

A Sophos Whitepaper. March 2023

Cybersecurity Challenges in the Education Sector

The cybersecurity challenges for the education sector continue to grow as the industry undertakes technological advancements, with more institutions turning to hybrid and remote teaching modes that increase vulnerabilities in the system. Besides this, cyber threats in this sector continue to grow in both volume and complexity.

A 2022 Sophos survey of 320 IT professionals working in lower education and 410 in higher education revealed that 56% of lower education and 64% of higher education organizations were hit by ransomware in 2021, compared to 44% of education respondents a year before. Education experienced the highest impact of ransomware on its ability to operate and its revenue/business compared to other sectors. The ransomware remediation costs in lower and higher education organizations were high: US$1.58M and US$1.42M, respectively.

Compounding the problem is the sector's slow ransomware recovery: 40% of higher education and 26% of lower education institutions took over a month to recover after being hit by ransomware. Besides the high level of ransomware attacks, the sector witnessed an increase in the broader threat environment: close to half of the education respondents reported an increase in the volume, complexity, and impact of cyber attacks on their organizations.

56% of lower education
64% of higher education
organizations hit with ransomware in 2021

$1.58M of lower education
$1.42M of higher education
average cost to remediate following an attack

>1 Month
26% of lower education and 40% of higher education organizations took over a month to recover following an attack

94% of lower education
97% of higher education
organizations hit by ransomware said it impacted their ability to operate

50%
of IT pros in education sector observed an increase in the complexity of attacks

62% in lower education
61% higher education
data recovered after paying the ransom

72% in lower education
74% in higher education
attacks on organizations resulted in data being encrypted

2%
of education sector organizations recovered ALL data after paying the ransom

Source: Sophos' global survey on The State of Ransomware 2022

Behind these statistics are several changes in the threat landscape:

The professionalization of cybercrime

Over the last year, one of the most significant developments has been the development and professionalization of the cyber threat economy. Criminal groups increasingly specialize in a particular component of an attack, for example, initial access, ransomware, information-stealing malware, and more, and offer it as a service to other criminals. These 'as-a-service' models lower the skill threshold required to conduct an attack, increasing the volume of adversaries and threats.

These specialist services provide execution guidance and resources for their criminal customers, enhancing the effectiveness of the attacks. Illustrating this point, in March 2022, an associate of the Conti ransomware-as-a-service group published an archive that included a rich trove of documentation and guidance designed to instruct an "affiliate" attacker in the steps required to conduct a ransomware attack.

Attackers are also adopting many of the behaviors of legitimate IT service providers, including asking ransomware victims to 'rate their service' once they have decrypted the files post-payment.

The evolution of attacker tactics, techniques, and procedures

Adversaries frequently exploit weaknesses in organizations' security posture to avoid being stopped by security solutions. These include:

- **Exploiting unpatched vulnerabilities** – This was the number one method adversaries used to penetrate organizations in attacks that Sophos' incident responders were brought in to remediate last year, used in 47% of incidents.
- **Exploiting legitimate IT tools** – Many of the top tools used by IT professionals are also abused by adversaries, including PowerShell, PsExec, and PowerShell, to exploit stolen access data and credentials. By posing as legitimate users, attackers hope to trick their way into an environment.

The cybersecurity challenges for this sector don't end here. The education sector must cope with threats like data theft of personal details of students, faculty, and other staff; espionage of valuable research and intellectual property data; DDoS attacks disrupting the continuity of operations; and phishing attacks that trick a student or faculty and redirect them to a wrong website, among other challenges.

Sophos Security for the Education Sector

Sophos delivers advanced cybersecurity solutions that enable educational institutions to manage and reduce cyber risk. Our adaptive cybersecurity ecosystem provides a complete portfolio of market-leading services and products that elevate our customers' defenses against even the most advanced threats, all powered by the unparalleled threat, AI, and security operations expertise of Sophos X-Ops.

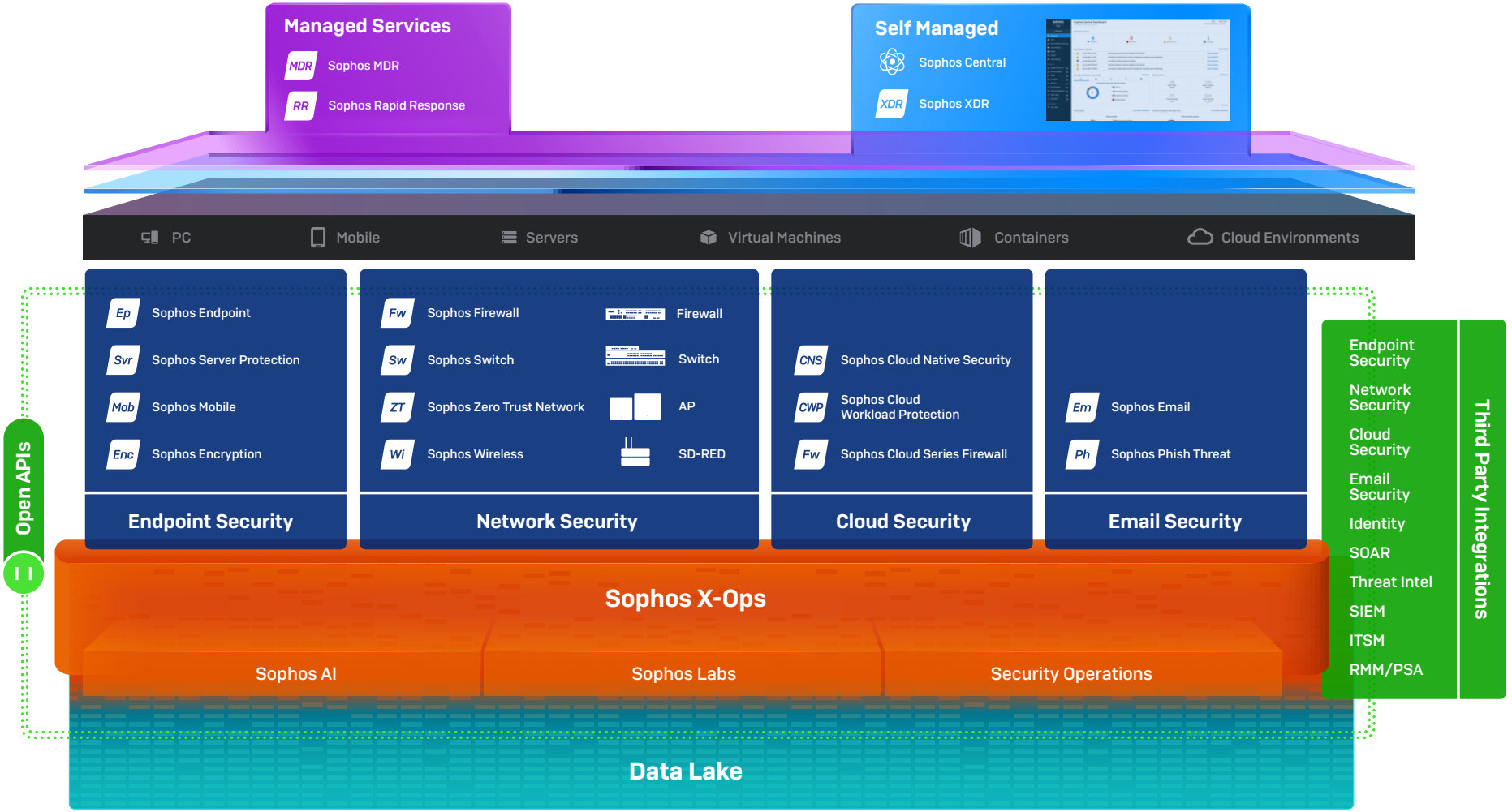
Sophos delivers leading cybersecurity outcomes for over **530,000 customers** globally.

No vendor has been **named a Gartner Leader** in endpoint security more times than Sophos.

The **highest rated** and **most reviewed** MDR Service, Endpoint and Firewall on Gartner Peer Insights.

As of August 1, 2022

Sophos Adaptive Cybersecurity Ecosystem



Use Cases

Sophos can help address the most common cybersecurity challenges facing the education sector.

Stopping advanced human-led attacks, including ransomware

Sophos MDR is a fully-managed, 24/7 service delivered by experts specializing in detecting and responding to cyberattacks that technology solutions alone cannot prevent. Our expert team stops advanced human-led attacks on your behalf, neutralizing threats before they can disrupt business operations or compromise sensitive customer data.

"The pen testers were shocked they couldn't find a way in. That was the point we knew we could absolutely trust the Sophos service."

University of South Queensland

"Since implementing Sophos, we've managed to free up significant operational hours that have allowed our teams to focus on initiatives that have increased our student satisfaction."

London South Bank University

"The Sophos team acts as our goalkeepers, sitting behind us with their skill sets and giving us reassurance that they have our back."

Inspire Education Group

With Sophos MDR, our expert analysts detect and respond to threats in minutes – using your preferred technology – whether you need a full-scale incident response or assistance making more accurate decisions.

We use:

- Sophos' award-winning solutions, including our endpoint, firewall, cloud, and email protection
- Products from other vendors such as Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, and many others
- Any combination of our technology and other vendors' technology

Sophos MDR protects your organization from advanced attacks that technology solutions alone cannot prevent while increasing the return on your existing investments. As the world's most trusted MDR provider, we have unparalleled depth and breadth of expertise in threats facing the education sector. Leveraging this extensive telemetry, we can generate 'community immunity,' applying learnings from defending one education customer to all other customers in the industry, elevating everyone's defenses.

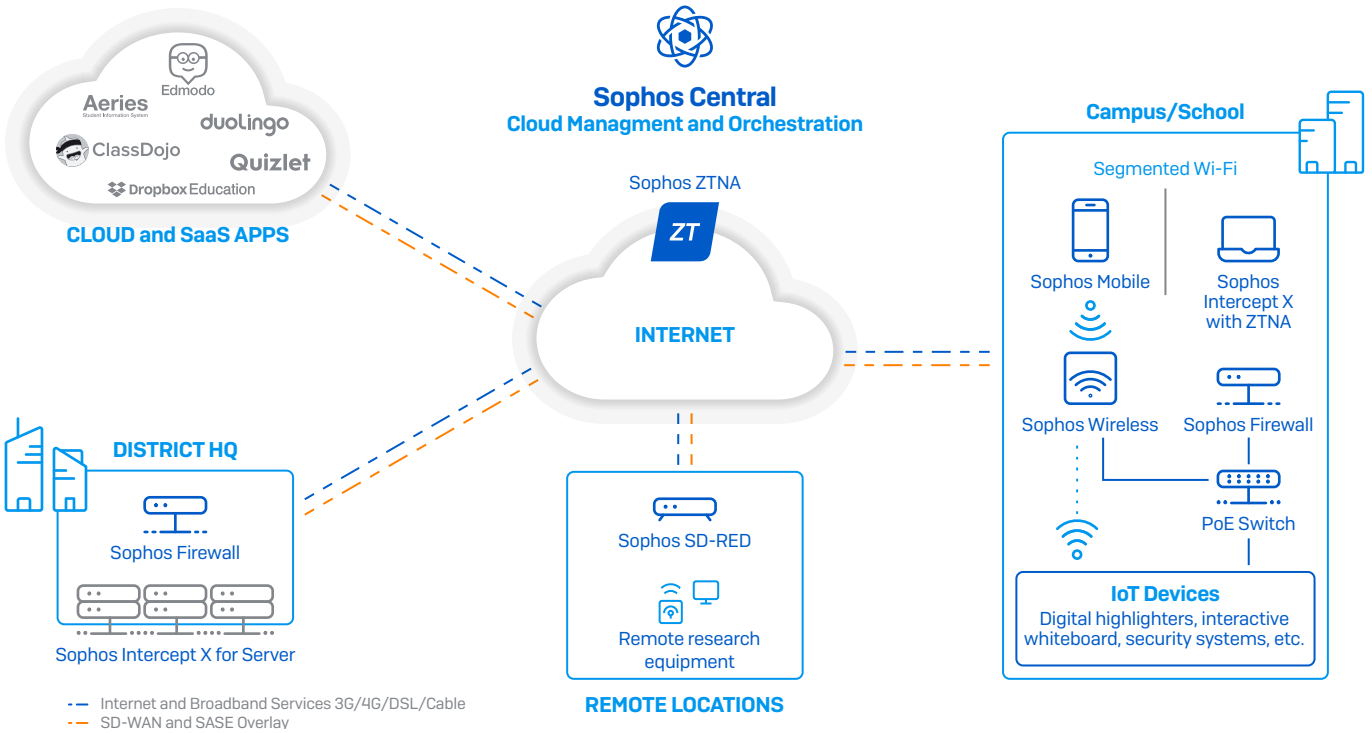
MOST TRUSTED	TOP RATED	BEST PROTECTION
#1 Provider	**4.8/5** Gartner Peer Insights	**38 mins** to detect, investigate, respond
More organizations trust Sophos for MDR than any other vendor	Highest-rated and most reviewed MDR solution as of August 1, 2022	Our analysts are over 5X faster than the fastest in-house SOC teams

As of September 2022

Securing branch and remote sites

Schools and colleges have moved beyond conventional classrooms to technology-driven "digital classrooms." The remote learning mode requires cloud-hosted collaboration tools, interactive displays like whiteboards, learning and assessment tools, and more, made available at high speed and performance. School districts and universities must securely connect different departments and sites to secure the exchange of personal data and digital teaching content, financial transactions, and more. The continued growth of new devices accessing the network – private and school-issued, must be managed and keep pace with upcoming educational technologies and apps on the network.

Sophos can help educational institutions to connect remote and branch sites; deliver critical cloud and SaaS applications like Dropbox Education, G Suite, ClassDojo, and others; and share data and information between sites with Sophos Secure Access portfolio. It includes Sophos ZTNA to support secure access to applications, Sophos SD-RED remote Ethernet devices to extend your network to branch locations and remote devices safely, Sophos Wireless access points for easy and secure wireless networking, and Sophos Switch for secure access on the LAN. Everything is managed through a single cloud-based security platform – Sophos Central.



Securing the endpoints of students and staff

Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – with Sophos Intercept X Endpoint, our market-leading EDR solution.

With cybersecurity, there is no silver bullet or single protection capability to stop every threat. Each attack combines a different set of tactics, techniques, and procedures (TTPs), and as a result, there is no 'one size fits all' protection solution. To optimize your defenses, you need layered protection: multiple sophisticated security capabilities, with each playing its part in defending against advanced attacks. Sophos Endpoint is packed with these layers of protection, including:

- Credential theft protection that prevents unauthorized system access.
- Exploit protection to stop the techniques adversaries use.
- Anti-ransomware protection, which identifies and blocks malicious encryption attempts.
- Tamper protection that prevents adversaries from turning off defenses so they can deploy their payloads.

Combining multiple layers of protection technologies enables us to optimize our customers' defenses. Testament to the quality of our defenses – and the power of layered protection – we stop 99.98% of threats up-front (AV-TEST average score) and recently earned perfect scores in SE Labs endpoint protection report.

Securing your network

Sophos Firewall includes features purpose-built for the education sector to offer robust protection from the latest threats while accelerating your important SaaS, SD-WAN, and cloud application traffic. Recognized as a Gartner Customers' Choice for Network Firewalls 2022, Sophos Firewall tightly integrates a full suite of modern threat protection technologies that are easy to set up and maintain.

- Powerful Web Filtering Policy

Utilize built-in policies for CIPA compliance and other education-specific features for SafeSearch and YouTube control.

- Child Safety and Compliance

Get compliant immediately with our built-in policy settings and essential features to monitor activity online.

- Context-aware Keyword Filtering

Identify problematic behavior like bullying before it becomes a real issue.

- Chromebook Support

Adds to our extensive user authentication options to enable full user-based policy and reporting on every platform.

- Top-Rated Protection from Threats

Ensures you are not wasting time cleaning up malware outbreaks or recovering from ransomware.

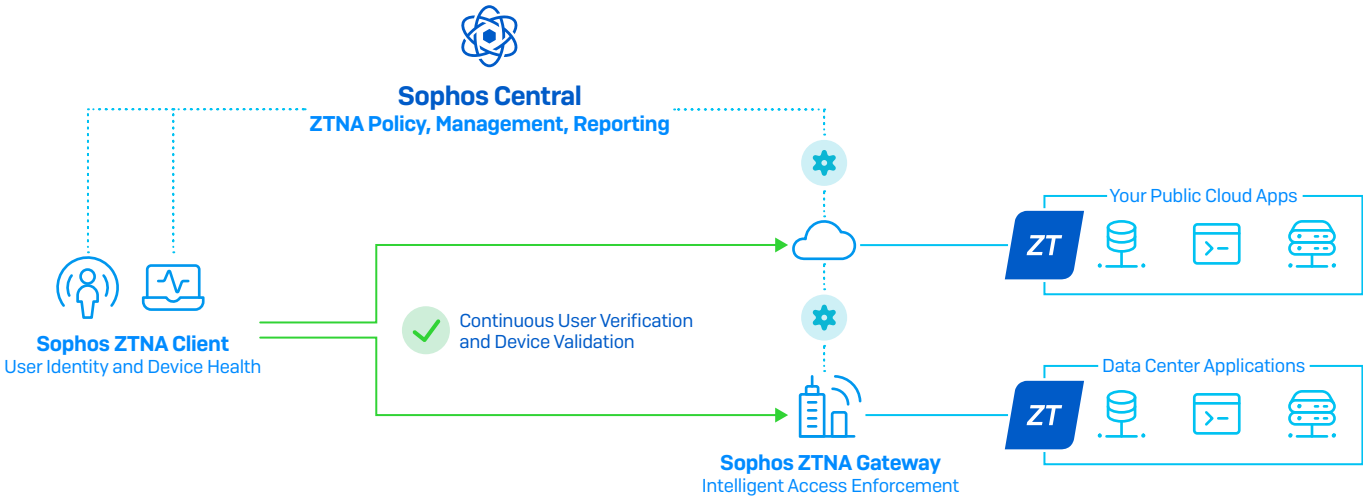
Securing research and personal data of students and staff

Schools and universities hold vast volumes of research data, with multiple departments requiring access to data. Furthermore, they collect and process personal and sensitive information about prospective and enrolled students and staff, including their financial and health records, legal guardianship, payment information, etc.

With thousands of users – students and faculty, connecting to their online portals across a multitude of devices during all times of the day, educational institutions need to adopt a zero-trust approach of trust nothing, verify everything to secure access to their sensitive data and critical intellectual property. Sophos' Zero Trust Network Access continuously validates user identity, device health, and compliance before granting access to applications and data.

The unique 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.

Data on users' endpoints operating on Windows, Mac, Linux, and virtual machines can be secured with Sophos Endpoint protection. It stops the latest cybersecurity threats to 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 via email, uploads, and local copying.



Identifying risky users in the system

Sophos Firewall helps you identify top-risk users based on recent web activity, threat, and infection history. A user's risk score can help you detect unintentional actions due to a lack of security awareness or a rogue or negligent user, indicating potentially problematic behavior early on. Sophos Firewall can log, monitor, or even enforce policies related to keyword lists related to 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.

Decrypting TLS/SSL traffic to maintain a safe learning environment

Tools that facilitate the exchange of resources and collaboration between teams are in high demand in schools and colleges. But nearly all of them, including the internet search engines like Google and SaaS applications like G Suite, Office365, and Dropbox, use encryption security protocols. Encrypted network traffic while offering protection, blinds network security and application monitoring tools. Cybercriminals use encryption to conceal malware, sneak hijacked data, cloak data exfiltration operations, and hide command-and-control traffic.

You cannot secure what you cannot see. Educational institutions must be able to see the encrypted traffic to control it and maintain a safe learning environment. Without visibility into encrypted traffic, web filtering solutions cannot detect and block inappropriate web activity. Students can bypass proxy servers to use unapproved apps and view content that may be harmful without being detected.

Unfortunately, most firewalls lack scalable TLS crypto capabilities and cannot inspect encrypted traffic without causing applications to break or degrade network performance. Sophos Firewall, with its new Xstream SSL inspection engine, fully enables TLS Inspection without compromising performance, protection, privacy, and user experience. It offers flexible policy tools to make intelligent decisions about what should and can be scanned, offloading where appropriate with a much higher capacity for concurrent connections.

Ensuring child safety and compliance

Sophos Firewall provides built-in features and policy settings that help organizations become compliant with local regulations quickly and easily. Sophos Firewall includes 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 to enable child safety online.

Securing resources in the cloud

The cloud is making classrooms innovative and genuinely collaborative. It offers easy access to students and faculty to resources across multiple platforms, anywhere and anytime. Educational institutions save significant money by shifting to the cloud as the costs of hardware and licenses are eliminated. However, the cloud is also an important target for cybercriminals looking to exploit less established cybersecurity practices than in traditional on-premises environments.

Sophos Cloud Native Security provides complete multi-cloud security coverage across your environments, workloads, and identities. It protects your cloud infrastructure and data with flexible host and container workload security for Windows and Linux. Multi-layered technologies protect against ransomware and other advanced attacks, including cloud-native behavioral and exploit runtime detections that identify threats such as container escapes, kernel exploits, and privilege-escalation attempts. It also makes it easy to keep on top of your cloud spend. You can quickly identify if your account is being abused and eject the adversaries before they rack up a hefty bill.

Conclusion:

Cyberattacks like ransomware, exploits, and phishing can have a severe business and reputational consequences for educational institutions. Protecting your IT environments and sensitive data requires an integrated security approach.

Sophos protects your systems and data wherever they exist with our next-gen services and technologies while enabling you to consolidate your security management with a single vendor. All Sophos solutions are controlled through a unified cloud-based management console, Sophos Central, which allows real-time information sharing between products, centralized management, automated incident response, and deeper insights – all of which, working together, further elevates your protection while enhancing the efficiency of your IT team.

To learn more about how Sophos secures educational institutions and to discuss your requirements, contact your Sophos representative or request a call-back from our security specialists.

2023-03-02 EN-WP (NP)

SOPHOS