SOPHOS

# Securing Higher Education Against Advanced Cyberthreats

## Sophos MDR is the leading Managed Detection and Response service for the education sector

Higher education providers such as colleges and universities are a prime target for cybercriminals. Adversaries are increasingly attracted by the valuable and sensitive information they hold, and the opportunity to extort payments using ransomware and the threat of breach exposure.

As cyberthreats grow in both volume and complexity, many higher education providers are turning to the Sophos Managed Detection and Response (MDR) service for protection against advanced attacks that technology alone cannot prevent. This solution brief explores the cybersecurity challenges facing the sector and introduces Sophos MDR, the number one MDR service supporting higher education today.

*A Sophos Whitepaper. February 2023*

# The Cybersecurity Challenge Facing Higher Education

## Higher education is a major target for cyberthreats

Almost two-thirds (64%) of higher education providers were hit by ransomware in 2021. In comparison, across the education sector as a whole, 44% of organizations fell victim to an attack in 2020[1]. This 45% rise over the course of a year demonstrates the rapid acceleration of the cyberthreat challenge facing the education sector.

More broadly, the majority of IT managers within higher education reported an increase in the volume (53%), perceived complexity (50%) and impact (50%) of cyberattacks over the last year. As cyber criminals continue to leverage automation and the 'malware-as-a-service' model in their attacks, these numbers are only set to increase.

**64%** hit by ransomware in 2021

**53%** report an increase in attack volume

**50%** report an increase in attack complexity

**50%** report an increase in the impact of cyberattacks

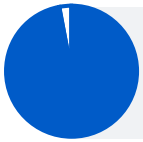
## The impact of advanced cyberthreats on higher education is severe

A major cyber incident has very considerable financial and operational repercussions for higher education providers. In 2021, the average ransom paid by the sector was a crippling $905,000. While this includes a small number of very large payments, almost one quarter (24%) paid between $50,000 and $100,000. Furthermore, the average overall cost to remediate a ransomware attack came in at $1.42 million, with well over one third (39%) of the encrypted data remaining unrecovered after the incident.

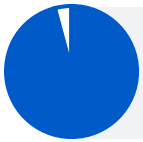
Recovery costs are just part of the story. Nearly all (97%) higher education establishments hit by ransomware said the attack impacted their ability to operate, while 96% of those in the private sector said it caused them to lose business/ revenue. In both cases, these are the highest impact figures reported across all industry sectors. If IT systems go down, providers' ability to deliver teaching and learning is often severely inhibited, with major repercussions for students and staff.

Compounding the challenge, higher education reported the slowest ransomware recovery across all sectors with only 60% of victims fully recovered one month after the attack; 31% required 1-3 months to recover and 9% reported a recovery period of 3-6 months.

**US$1.42M** ransomware recovery cost



**97%**
of attacks impacted ability to operate



**96%**
of attacks resulted in lost business/ revenue (private sector only)

1 The State of Ransomware in Education, 2022, Sophos. Independent survey of 5,600 IT professionals including 410 from higher education establishments. Hit by ransomware is defined as one or more devices being impacted but not necessarily encrypted.

## Higher education is struggling to keep pace with well-funded adversaries

The reality is that technology solutions alone cannot prevent every cyberattack. To avoid detection by cybersecurity solutions, malicious actors increasingly use legitimate IT tools, exploit stolen credentials and access permissions, and leverage unpatched vulnerabilities in their attacks. By emulating authorized users and taking advantage of weaknesses in an organization's defenses, malicious actors can avoid triggering automated detection technologies.

The only way to reliably detect and neutralize determined cyber attackers is with 24x7 eyes on glass delivered by expert operators who leverage diverse security alerts and real-time threat intelligence to identify and stop threats before the damage is done.

However, the complexity of modern operating environments and the velocity of cyberthreats make it increasingly difficult for most organizations to successfully manage threat detection and response on their own. Illustrating this point, the average intruder dwell time in the education sector was 34 days,  more than double the 15-day cross-sector average[2].

Organizations across all sectors, including higher education, are struggling to keep pace with well-funded adversaries who are continuously innovating and industrializing their ability to evade defensive technologies.

2 The Active Adversary Playbook 2022, Sophos - Report is based on 144 incidents targeting organizations of all sizes in a wide range of industry sectors

# Sophos MDR: Securing Higher Education

As the cybersecurity challenge continues to grow, higher education providers are increasingly turning to the Sophos MDR service to help them stay ahead of today's advanced threats.

## 24/7/365 ransomware and breach prevention service

Sophos Managed Detection and Response (MDR) is a fully managed service delivered by experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more.

- **Detect:** We monitor your environment 24/7, collecting, contextualizing, and correlating security data from the Sophos Adaptive Cybersecurity Ecosystem and your existing cybersecurity investments to identify suspicious activities
- **Investigate:** Expert human operators investigate potential incidents, leveraging our deep education sector and threat expertise to hunt for signs of adversarial activities
- **Remediate:** Analysts quickly remediate attacks across the broad range of your environment, before they turn into something more damaging such as ransomware or a wide scale data breach
- **Review:** Comprehensive root cause analysis of incidents together with regular health checks and weekly and monthly reporting enable you to improve security posture and prevent future recurrence

With an average time to detect, investigate and remediate of just 38 minutes, Sophos MDR is more than 5 times quicker than even the fastest in-house security operations team.

With Sophos MDR, you benefit from our team of over 500 security operations specialists who provide expertise across all elements of the detection and response cycle, from threat hunting and neutralization to malware engineering and security automation. With six security operations centers (SOCs) located across Australia, India, Europe, and North America, we provide seamless 24/7 coverage every day of the year.

## A service designed around you

We understand that each higher education provider is different with their own existing security investments, IT/cybersecurity staff, and IT environment. Sophos MDR meets you where you are: you choose the level of support required, whether you want us to notify you of threats so your team can take remedial action, contain threats on your behalf, or provide full incident response and root cause analysis. Our security specialists will work with you to identify the right approach for your organization.

## Elevate your protection using your existing investments

Today's advanced threats can come from any direction, and adversaries often deploy multiple tools, tactics and procedures in the course of their attacks. Sophos MDR analysts detect and respond to attacks across your entire environment using the Sophos and third-party security tools you already have in place. We can use your:

- **Endpoint telemetry** to spot malicious activities and attack behaviors
- **Firewall data** to detect intrusion attempts and beaconing
- **Network telemetry** to identify rogue assets, unprotected devices, and novel attacks
- **Email alerts** to pinpoint initial entry into the network and attempts to steal access data
- **Identity data** to detect unauthorized network entry and attempts to escalate privileges
- **Cloud alerts** to indicate unauthorized network access and efforts to steal data

The more we see, the faster we act. By detecting and responding to advanced attacks using your existing security tools, Sophos MDR reduces cyber risk while increasing return on your security investments.

# Sophos MDR: The Number One MDR Service For Higher Education

Sophos is the number one MDR provider globally, securing more organizations than any other provider against ransomware, breaches, and other threats that technology alone cannot stop.

Sophos MDR secures hundreds of education organizations, giving us unparalleled depth and breadth of expertise into threats facing the higher education sector. We leverage this extensive telemetry to generate 'community immunity', applying learnings from defending one provider to all other customers in the sector, elevating everyone's defenses.

Of course, what matters most is the cybersecurity outcomes we deliver for our customers. Sophos is the highest rated and most reviewed MDR solution on Gartner® Peer Insights™ with a 4.8/5 rating across 271 reviews as on December 20th, 2022 and 97% of customers saying they would recommend us. Sophos is also rated the Top Vendor in the 2022 G2 Grid® for MDR Services serving the midmarket, as well as being named a Leader for MDR in the G2 Overall, Midmarket and Enterprise segments.

## Number 1 for Higher Education

- ✓ **Most trusted:** over 15,000 organizations use Sophos MDR
- ✓ **Highest rated:** 97% of customers would recommend us
- ✓ **Most reviewed:** 271 reviews on Gartner Peer Insights in 2022

## Hear from our education customers

★★★★★

*"The MDR team disabled the threat, reported the findings to us, and included the username, workstation ID, and the type of drive used. I was able to inform the employee of the problem so it did not happen again. Overall, we are very pleased with their services."*

<5000 Employees, North America. Full review on Gartner Peer Insights

★★★★★

*"Overall satisfied with product performance and service capability of Sophos MDR."*

<5000 Employees, Asia-Pacific. Full review on Gartner Peer Insights

★★★★★

*"We are using Sophos MDR Service and it is very helpful to cater our cybersecurity needs. We also find it difficult to comply with regulations such as the Children Internet Protection Act (CIPA) and General Data Protection Regulation (GDPR) but after opting Sophos Solution we are complying on these guidelines."*

<5000 Employees, Asia-Pacific. Full review on Gartner Peer Insights

★★★★★

*"Sophos MDR is life saviour solution for an IT organization whose 24 /7 threat hunting detection and response gives proactive protection with any sophisticated and malicious threat."*

<5000 Employees, EMEA. Full review on Gartner Peer Insights

# Next Steps

To learn more about Sophos MDR and how we can support your organization, speak with a Sophos adviser today or visit www.sophos.com/mdr

*"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

## Sophos MDR

- 24/7 real-time threat monitoring and response
- Expert lead threat hunting
- Cross-product (Sophos and third-party) consolidation and correlation of security event data
- Full-scale managed incident response (unlimited number of hours; no additional fees or retainers)
- Best in class breach protection warranty
- Dedicated incident response lead assigned
- Direct call-in support to Sophos security operations centers (6 global SOCs)
- Weekly and monthly activity reports
- Monthly intelligence briefings
- Root cause analysis performed to improve security posture and prevent recurrence of future threats
- Regular Sophos account health checks to review configurations and ensure optimal performance



2023-02-09 (WP-NP)

SOPHOS