WHITEPAPER

ThreatDown™
Powered by Malwarebytes

IS MDR RIGHT FOR YOUR DISTRICT?

An Assessment of MDR's Value Proposition for Primary and Secondary Schools

Contents

INTRODUCTION

In the winter of 2022/23, the Department for Science, Innovation and Technology (DSIT) conducted the eighth Cyber Security Breaches Survey, featuring an annex devoted to education.[1] The results are disheartening.

Among other findings, results indicate that education institutions continue to be targeted by cyber criminals: All education institutions were more likely to report cyber security breaches or attacks in the last 12 months than the average UK business.[i]

In fact, only 32 per cent of UK businesses reported breaches or attacks (down from 39 per cent in 2022). Meanwhile, at 41 and 63 per cent, respectively, primary and secondary schools fared far worse in 2023 than UK businesses.[ii]

Results from a different audit within the same timeframe are equally saddening. In May 2022, the London Grid for Learning (LGfL) and the National Cyber Security Center (NCSC) surveyed schools throughout the UK. Of the 805 participating schools, nearly half reported that they "do not feel prepared" for a cyber attack—and less than half have a business continuity plan that covers a cyber breach or attack.[iii]

Cyber attacks against schools can disrupt learning, shut down access to critical systems, and cost a lot of money—with or without succumbing to a ransom demand. In January 2023, attackers demanded £15 million in ransom from at least 16 secondary schools hit over the winter holidays.[iv] And September 2023 seemed to bring a spate of attacks against UK schools, forcing many to delay start times.[v]

What is perhaps most disconcerting is that *no* school is immune. The Harris Foundation, a charity responsible for 52 primary and secondary academies that serve ~40,000 disadvantaged children, was attacked by a ransomware gang in 2021. When the multi-trust academy (MAT) refused to pay the £3 million ransom (that doubled during negotiations), attackers retaliated by releasing confidential data of the academy chain's 38,000 pupils. Despite their refusal to pay, the MAT spent £500,000 to recover.[vi]

Primary and secondary schools are prime targets because they store valuable data[2] and are widely-known to have budget constraints. Unlike businesses, schools have small (to non-existent) security operation centers (SOCs) with few (or no) highly-skilled cyber security professionals.

This lack places the figurative school branch, weighted with the valuable data that is its fruit, at an enticing level that invites easy picking.

> *Nearly half of schools do not feel prepared for a cyber-attack and less than half have a business continuity plan that outlines next steps in the event of an incident."*
>
> **– "Cyber security in schools – are we teaching and learning?"**
> 2022 audit of cyber security in UK schools, LGfL

ACE CYBER SECURITY

If your school is like most, you likely need to improve its cyber security posture and will explore several avenues to determine how best to do so.

Options abound, of course, but schools have unique challenges they must factor into their decision. For example, schools must ask whether their IT team has the staff and skill necessary to deploy, configure, and manage any solution they consider.

One option for cyber security that seems particularly well suited for schools is managed detection and response (MDR).

MDR is a turnkey service that delivers an as-a-service SOC that combines provider-specific detection and response technology with a team of experienced cyber security analysts. These analysts are dedicated round-the-clock to protecting their clients through monitoring, proactive threat hunting, and incident management.

With MDR, organisations accelerate threat detection, analysis, investigation, and response, which can include automated and managed threat containment and mitigation. MDR can be an affordable solution and should be tailored to meet your school's cyber security needs.

But is MDR right for your school? The goal of this paper is to help you answer that question by prompting you to consider these five smaller ones:

1. Does your security team lack sufficient staff to deliver 24/7 services?
2. Does your security team have the time and skill to stop attacks?
3. Is your security team overwhelmed by seemingly endless alerts?
4. Do you need to mitigate the risk of regulatory violations?
5. Can you justify the expense of MDR for your school?

> *… All too frequently schools sign up (and pay for!) A [cyber security] solution but don't activate all its features or install it on all devices. Equally, once it has been deployed, someone needs to keep an eye on it! … the expression 'set and forget' may be catchy, but it is dangerous!""*
>
> **– "Cyber security in schools – are we teaching and learning?"**
> LGfL and NCSC

#1 | DOES YOUR SECURITY TEAM LACK SUFFICIENT STAFF TO DELIVER 24/7 SERVICES?

If the team that monitors your school's cyber security is operational only 40 to 50 hours per week, then your school is at an increased risk for a ransomware attack: the majority (76%) of ransomware attacks take place either on week nights (49%) or over the weekend (27%).[vii]

Holidays also invite an increase in cyber incidents, as observed by the US Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency.[viii] In the UK, we've experienced evidence of this claim only this year: In January 2023, 16 primary and secondary schools reported having been attacked over the holidays.[ix]

To offset 24/7 threats, it stands to reason that you need 24/7 security. Leaving your schools without cyber security supervision during evenings, weekends and holidays is a bit like leaving your house unlocked when you're away.

Unfortunately, your school might lack the cyber security staff necessary for delivering security services 24/7.

If you answer "Yes" to #1....

If your security team is inadequately staffed, then MDR might be a sensible choice for you.

Partnering with an MDR service provider enables you to:

- maximize your cybersecurity posture on a 24/7 basis—starting now—without the expense (and hassle) of hiring staff to do so; and
- free up time for your security team to turn attention toward critical projects, such as conducting digital forensics, training faculty, staff and students on cybersecurity policies, and fine-tuning procedures that ensure ongoing compliance.

> *Between April 2022 and March 2023:*
>
> - *The UK was the second most attacked country in the world*
> - *Royal Mail was hit with the largest known ransom demand: $80 million*
> - *The UK education sector was hit far harder than education in other countries*
> - *The UK was a prime target for Vice Society, which sets its sites on education*
>
> **– ThreatDown Threat Intelligence**[x]

#2 | DOES YOUR SECURITY TEAM HAVE THE TIME AND SKILL TO STOP ATTACKS?

In cyber security, dwell time refers to the hours, days, or months that attackers lurk undetected in your network; it's the time between access and discovery. Ideally, dwell time would be measured in minutes—or, even better, seconds: The attack would be spotted immediately and contained before it could do harm.

But schools don't live in this ideal world—and they're not alone in the real world. According to 2022 research from Ponemon Institute and IBM Security, the average time for organisations across all industries to identify a breach is 207 days; it takes organisations another 70 days to contain the breach.[xi] 277 days is a long time and a far cry from the end goal of cyber security, which is to stop an attack.

To help manage the continual onslaught, your school may have deployed an endpoint detection and response (EDR) solution. EDR is the de facto cyber security standard for endpoint protection. When properly configured, EDR can find both known and unknown threats and automate responses (such as quarantining suspicious code).

An EDR solution offers a solid start to protecting network data. But without experienced cyber security analysts dedicated to the task of monitoring that solution, the protection it provides can fall short of your needs.

Your team is already overwhelmed by mundane IT issues, which leaves little time for adequate monitoring. Your team might also struggle to configure EDR to flag the right types of threats—without inadvertently configuring it to trigger alerts for everything.

Your team might also lack the experience it takes to investigate and analyze EDR log files (or "telemetry"). EDR telemetry contains clues that seasoned professionals recognize and use to uncover indicators of compromise (IoCs), among other things.

If you answer "Yes" to #2....

The power behind MDR is that it starts with the automated detection and response that EDR offers—but it doesn't stop there.

With MDR, you partner with a team of experienced analysts who are dedicated to monitoring their clients' EDR logs, which to the inexperienced can appear arcane. An MDR team of seasoned threat hunters may have years or even decades of experience analyzing telemetry to find and stop attacks that software—no matter how advanced—can miss.

MDR threat hunters can do what the most sophisticated software cannot: they can stop the *people* behind an attack, not just the malware those people are deploying.

> *"Given the global shortage of skilled, experienced cyber security professionals, even large corporations struggle to recruit and retain cyber security staff. So what hope is there for cash-strapped schools...?"*
>
> **– "Cyber security in schools – are we teaching and learning?"**
> 2022 audit of cyber security in UK schools, LGfL

With MDR, you gain a team of experienced threat hunters who vastly improve your cyber security posture with feats such as these:

- uncovering a brute force attack against a remote desktop protocol port by poring over telemetry;
- recognizing a pattern of unfamiliar activity coming from a single account (indicating potential compromise);
- creating a rule to block activity they recognize as ransomware—before this new variant has even been identified and named by groups like CISA or MITRE ATT&CK.[3]

#3 | IS YOUR SECURITY TEAM OVERWHELMED BY SEEMINGLY ENDLESS ALERTS?

Ideally, school teams investigate all of the risk alerts that EDR and other cyber security systems trigger.

But the volume of these alerts can be overwhelming. Small teams struggle to find and promptly address critical alerts while avoiding wasting time on less *critical* (or even false) alerts.

If they had money to spare, schools would probably hire more cyber security professionals to assist. Unfortunately, the ongoing global shortage of cyber professionals leaves schools short on the financial incentives it takes to attract and maintain these highly-sought-after experts.

Any team that is overworked is prone to burnout, which in the context of cyber security manifests as "alert fatigue." Alert fatigue is just what it sounds like: Exhaustion resulting from seemingly endless alerts and the effort of investigating them. Not surprisingly, 41 per cent of security alerts that *should* be investigated are ignored.[xii]

> *Alert fatigue ... happens to cyber security experts that get exposed to vast numbers of frequent alerts ... consequently desensitizing them to the warnings. It results in longer response times or missing important alerts or alarms."*[xiii]

If you answer "Yes" to #3....

Many districts have found it helpful to outsource alert monitoring to an MDR service provider.

By partnering with an MDR provider, you gain a team of experts, who sift through the overabundance of threat alerts to identify the top critical threats. Armed with this additional security expertise, your team:

- is less likely to miss critical threat alerts;
- gains back time wasted on investigating lower-level or false-positive threat alerts;
- gains more time to respond appropriately to threats that matter; and
- receives fewer alerts, which in turn, reduces the teams' susceptibility to alert fatigue.

#4 | DO YOU NEED TO MITIGATE THE RISK OF REGULATORY VIOLATIONS?

The stakes associated with cyber security (or lack thereof) involve more than the threats themselves: primary and secondary schools collect and process data that is safeguarded under one or more data protection regulations, such as the EU's General Data Protection Regulation (GDPR). Your school might need to verify compliance with data protection regulations.

Given the rising costs of protecting data and the exhorbitant costs of a breach, your school might also be ensured against these risks. DSIT 2023 cyber security breaches suvey reports that half (50 percent) of primary schools and nearly half (46 per cent) of secondary schools are insured against cyber risk.[xiv]

If your school is among this insured crowd, you likely need to prove that your cyber security mechanisms meet insurance requirements. Failure to provide evidence of meeting those requirements may increase your premiums or preclude cyber insurance altogether.

Apart from the risk of fines for regulation violations or increased cyber insurance premiums, your organisation's success depends on your community's trust. To help maintain that trust, you might need to provide evidence to a governing board of your efforts to protect the valuable data your school holds.

If you answer "Yes" to #4....

Partnering with an MDR will help you:

- comply with most data protection regulations by providing many of the critical steps required for doing so;
- meet cyberinsurance requirements; and
- maintain your community's trust.

> *Under GDPR, "schools are obligated to document and review all of the personal information they hold." Among other requirements, schools must:*
>
> - *Ensure staff are aware of GDPR, how data is collected and stored, and the implications of a breach*
> - *Ensure all software is GDPR compliant to avoid "serious fines"*
> - *Have a data protection officer, who is responsible for GDPR compliance and data protection*
>
> – **GDPR Compliance in Schools**
> Inside Government, Schools

#5 | CAN YOU JUSTIFY THE EXPENSE OF MDR FOR YOUR DISTRICT?

Your school has a fiduciary responsibility to be a good steward of funds. Every expense demands justification, and every justification must be linked somehow to providing an excellent learning environment for the students.

Can you justify the expense of MDR—and, if so, by what standard of measurement?

Justifying the necessity of improved protection should not be difficult. Point to the alarming increase in cyber security attacks. For example, ThreatDown Threat Intelligence Team found that between June 2022 and May 2023, the education sector worldwide experienced an 84 per cent increase in attacks.[xv]

Evidence of this clear and present danger should convince even the most cyber security illiterate of the need for always-current, always-available defenses. But that brings you no closer to justifying the expense of MDR in particular.

One way to justify the expense of MDR is to estimate its return on investment (ROI). Research suggests that for most educational organisations, MDR pays for itself in approximately two months, when you factor in the cost of internal staff.[xvi]

For example, at a cost of $3 per endpoint (for 24/7/365 monitoring, investigations, triage and remediation), a school with 1,000 endpoints would pay $3,000 per month. Now weigh that cost against the expense of hiring and maintaining inhouse cyber security professionals to work the same hours and accomplish similar tasks. A scenario such as this yields an ROI of as much as 425% with a payback on MDR in 2.3 months.[xvii]

In addition, by some estimates, MDR reduces the risk of a breach by 99%.[xviii] When you consider that statistic against the cost of recovering from a breach—which by some estimates averages US $2.73 million for education[xix] —deploying MDR seems a sensible choice indeed.

If "Yes," Then MDR Is a Sensible Option

To assess whether MDR makes financial sense for your school, run a risk assessment, calculate the ROI, and see where you stand.

MDR improves your cyber security posture quickly, dramatically reduces your risk of breach, and potentially:

- reduces time-to-value for, and
- increases the ROI of security.

> *The only way to secure budget is to outline the worst-case scenario. You've got the personal data of 600 children, staff bank accounts and addresses, [and] medical records; you can lose access to your entire network and not be able to teach."*
>
> **– Secondary school as quoted in "Cyber security breaches survey 2023"**

CONCLUSION

If you answered "Yes" to one or more of the above five questions, then partnering with an MDR provider is likely a sensible choice for your school. Not surprisingly, MDR is growing in popularity faster than other cyber security options: In a 2023 market guide for MDR, Gartner estimates that 60 per cent of organisations worldwide will be using MDR services by 2025, up from 30 per cent today.[xx]

Given its increasing popularity, MDR might raise the bar for baseline security. If so, then not partnering with an MDR provider could leave your school well below the baseline bar—like enticingly low-hanging fruit.

> *If having excellent security training and firewalls is like having an iron fence and security guards outside your house from 9 to 5, then MDR represents a group of martial artists inside your house watching every window 24/7."*[xxi]
>
> **– Peter Casserly**
> Casserly Consulting

THE IDEAL MDR PARTNER

Ready to find your ideal MDR partner? Here are two critical areas to discuss with prospective MDR partners.

#1 The MDR technology stack: Each MDR provider has a unique technology stack, which is provider-owned and -managed. This stack should continually monitor your environment to automatically detect, investigate, and remediate threats. For example, ask about the EDR solution: a good one will be effective and intuitive out of the box.

ThreatDown, powered by Malwarebytes', EDR is both effective and intuitive—and has the **MITRE ATT&CK 2022** results to support that claim. (See "Glossary of cyber security terms.")

#2 The MDR team: Each MDR provider will offer different degrees of collective experience; wouldn't you like to know what you're getting? Ask. MDR analysts should be experienced cybersecurity professionals with expertise in threat detection, analysis, incident response and, ideally, data regulation requirements and compliance issues.

The MDR team features cybersecurity professionals with decades of experience and a singular focus on this mission: to protect customers from cyber threats and remediate cyberattacks.

GET A QUOTE >

GLOSSARY OF CYBER SECURITY TERMS

Alert fatigue: a condition to which cybersecurity professionals are susceptible that is characterized by desensitization to overwhelming numbers of alerts; alert fatigue can lead to ignored or missed security alerts. See "fear of missing incidents (FOMI)."

Endpoint detection and response (EDR): a cyber security technology that continually scans an endpoint (e.g., laptop, PC, server) for the purpose of thwarting cyber attacks. An EDR solution should meet these three critical requirements:

1. Detect, isolate, prevent, and remediate threats
2. Investigate, threat hunt, and rollback ransomware
3. Deploy, manage, integrate, and report with ease

False positives: behaviors that incorrectly trigger an alert indicating the presence of a cyber security threat, which poses a serious problem for IT and security teams. According to the Enterprise Strategy Group, nearly half of all alerts are false positives.

Fear of missing incidents (FOMI): derived from FOMO (fear of missing out), FOMI is an anxiety or dread that some IT and security professionals experience because they simply cannot investigate all of the alerts they receive; closely related to "alert fatigue."

Indicators of Compromise (IoCs): clues or traces that attackers leave behind that show not only that a system intrusion or data breach has occurred but might also show how it happened and who is to blame. Unlike threat hunting, which can thwart an attack before it occurs, IoCs show you only what has already happened.

MITRE ATT&CK (for Adversarial Tactics, Techniques, and Common Knowledge): created in 2013 based on real-world observations, MITRE ATT&CK is a framework for describing and categorizing cyber attacks (according to their tactics and techniques). MITRE uses its ATT&CK framework to mimic known tactics and techniques as a way of testing and evaluating products.

Threat detection: a reactive search for IoCs to uncover what happened and who is to blame. Efficient threat detection is necessary for prompt incident response and remediation.

Threat hunting: a proactive search for threats aided by both machine learning (ML) tools and by trained security analysts. ML tools automatically and continually scan a network to observe user and device behaviors; the purpose is to detect anomalous and, therefore, suspicious behavioral patterns that might point to malware with an unknown signature. Once alerted, analysts investigate the potential risks to assess the validity of the ML tool's hypothesis.

Zero-day threats: software flaws that are vulnerable to attack and have not yet been patched.

Zero-day attack: an attack by way of an unpatched software flaw.

RESOURCES

[i] "Cyber security breaches survey 2023: education institutions annex," Department for Science, Innovation and Technology, 19 April 2023.
[ii] See i.
[iii] LGfL and NCSC, "Cybersecurity in schools – are we teaching and learning? Analysis and next steps from the 2022 audit of cybersecurity in UK schools," based on audit conducted from 3 to 31 May 2022.
[iv] Lodge, Matthew. (6 January 2023.) "Hacky new year!" *DailyMail*.
[v] Muncaster, Phil. (5 September 2023.) "More Schools hit by Cyber-Attacks Before Term Begins." *InfoSecurity Magazine*.
[vi] Gibbons, Amy, "MAT falls victim to data leak after $8m ransom demand," *TES Magazine*, 19 July 2021.
[vii] C. Cimpanu, "Most Ransomware Attacks Take Place During the Night or Over the Weekend," 16 May 2020.
[viii] Cybersecurity advisory (Alert Code: AA21-243A), "Ransomware Awareness for Holidays and Weekends," Cybersecurity & Infrastructure Security Agency, 10 February 2022.
[ix] See iv.
[x] Threat Intelligence Team, "Ransomware in the UK, April 2022-March 2023," Malwarebytes, 12 April 2023.
[xi] Ponemon Institute and IBM Security, "Cost of a Data Breach 2022," IBM Corporation, Armonk, NY, 2022.
[xii] "The State of Security 2023," Splunk, 2023.
[xiii] Techslang, "What is Alert Fatigue?" Cyber security Glossary.
[xiv] See i.
[xv] Malwarebyte Threat Intelligence, "The 2023 State of Ransomware in Education," Malwarebytes, 5 June 2023.
[xvi] Malwarebytes internal research.
[xvii] Malwarebytes internal research.
[xviii] Malwarebytes internal research.
[xix] S. Adam, "The State of Ransomware in Education 2021," 13 July 2021.
[xx] P. Shoard, Al Price and 3 more, "Market Guide for Managed Detection and Response Services," Gartner Research, 14 February 2023
[xxi] P. Casserly, "Why Every SMB Needs Managed Detection and Response," Casserly Consulting, 2020.

---

[1] Conducted since 2016, the 2023 Cyber Security Breaches survey was commissioned by the DSIT for the first time this year. In February 2023, responsibility for UK cyber security policy moved from the former Department for Digital, Culture, Media and Sport (DCMS) to the DSIT.
[2] Schools store student, staff, and teacher data that includes their National Insurance Number, Special Education Needs, immigrant status, gender race, and birthdate; they may also store passport scans, staff pay scales, and even bank details.
[3] CISA stands for the US Cyber Security and Infrastructure Security Agency, and MITRE is name of the organisation that maintains the ATT&CK list, which stands for Adversarial Tactics, Techniques and Common Knowledge

ThreatDown™ Powered by Malwarebytes | malwarebytes.com/mdr | corporate-sales@malwarebytes.com | 1.800.520.2796