Whitepaper

ThreatDown™
Powered by Malwarebytes

Is MDR Right For Your District?

An Assessment of MDR's Value Proposition for K-12

ThreatDown™ Powered by Malwarebytes

Contents

ThreatDown™ Powered by Malwarebytes

Introduction

Cybersecurity attacks against K-12 districts are increasing in volume and sophistication. In a September 2022 Cybersecurity Advisory (CSA) Alert, three government agencies[1] combined forces to warn K-12 institutions that they were being "disproportionately" attacked by a ransomware syndicate. The Alert adds that K-12 districts have been the "frequent target" of such attacks over the past several years, and the agencies fear an increase in these attacks.[i]

United States public schools have disclosed an average of more than one K-12 cyber incident per school day.[iii]

This is disheartening news—particularly given that the education sector already holds the unfortunate 2020 claim of having suffered more ransomware attacks than any other industry.[ii]

To uncover the impact of cyberattacks on K-12 districts, the U.S. Government Accountability Office (GAO) conducted its own extensive research. The GAO found that impacts include up to three weeks of closed schools, two to nine months for recovery, and direct monetary costs of $50,000 to $1 million.[iv]

What is arguably more disturbing is that compared to any other industry, the education sector paid the highest bill overall to recover from ransomware attacks. When incorporating all costs—including staff time, device and network repairs, ransom money, and downtime—education institutions shelled out US $2.73 million on average; 48% more than the global average.[v]

The CSA Alert and GAO report followed closely on the heels of a cyberattack against the second largest K-12 district in the United States: Los Angeles Unified School District (LAUSD). When the district refused to pay the ransom (at the advice of the FBI), the ransomware syndicate, Vice Society, leaked the 500GB of data it had managed to encrypt and steal. Vice Society posted LAUSD personal identifiable information (PII) to their site on the dark web, including staff and student passport details, social security numbers, and tax forms.[vi] PII, as you well know, is a lucrative commodity.

All of this alarming news begs the question: why are K-12 districts such attractive targets?

Metaphorically, the answer is that K-12 districts are low-hanging fruit that cybercriminals are inclined to pick. Large enterprises have money, which lends itself to a security operation center (SOC) with a budget conducive to buying and maintaining advanced security tools and enticing seasoned cybersecurity experts. This places large enterprises in the uppermost branches of the figurative fruit tree.

In contrast, K-12 districts are commonly funded with taxpayers' dollars, which leaves them with limited funds available for cybersecurity. Cybercriminals bank on the fact that K-12 districts have small (to non-existent) SOC teams with few (or no) highly-skilled cybersecurity professionals. And the weight of that burden bends the K-12 branch to an enticing level that invites easy picking.

ThreatDown™ Powered by Malwarebytes

From Low-Hanging to Unreachable at a Price Within Reach

Your district needs to improve its cybersecurity posture and will no doubt explore several avenues to do so. However, one avenue that calls for your consideration is managed detection and response (MDR).

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

With MDR, organizations 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 district's cybersecurity needs.

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

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

> *I have two cybersecurity people for 60,000 machines. We want to sleep and take holidays off. A good MDR can help with that for less than it would cost to staff the same thing yourself."*[vii]
>
> **– April Mardock**
> CISO and Ops Manager, Seattle Public Schools as quoted by Ed Tech Magazine Focus on K-12

#1 | Does your security team lack sufficient staff to deliver 24/7 services?

If the team that monitors your district's cybersecurity is operational only 40 to 50 hours per week, then your district 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%).[viii]

Holidays also invite an increase in cyber incidents. For example, studies show a 70% increase in ransomware attempts across all industries over the winter holidays.[ix] This shouldn't come as a surprise: cybercriminals likely guess that over the holidays, fewer IT professionals will be in the office.

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

Unfortunately, your district might lack the cybersecurity staff necessary for delivering security services 24/7. In fact, results from Project Tomorrow's 2021 research on the state of K-12 cybersecurity affairs suggests that if your district is like most, then it is likely short on staff. According to Project Tomorrow's survey results, "Nearly 6 in 10 [K-12] technology leaders say that their current staffing for cybersecurity is not adequate to meet the needs of their district to protect information assets and resources."[x]

> *[MDR] allows a higher level of expertise than you might have locally."*[xi]
>
> **– Amy McLaughlin**
> Cybersecurity Program Director, CoSN as quoted in Ed Tech Magazine Focus on K-12

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.

#2 | Does your security team have the time and skill to stop attacks?

In cybersecurity, 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 K-12 districts 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 organizations across all industries to identify a breach is 207 days; it takes organizations another 70 days to contain the breach.[xii] 277 days is a long time and a far cry from the end goal of cybersecurity, which is to stop an attack.

> *"Let's face it, threat detection and response requires advanced skills that most organizations don't have. Additionally, the technologies used for threat detection and response … can be expensive and complicated."*[xiii]
>
> **– Jon Oltsik**
> Principal Analyst, Enterprise Strategy Group (ESG)

To help manage the continual onslaught, your district has probably deployed an endpoint detection and response (EDR) solution. EDR is the de facto cybersecurity 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 cybersecurity 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.

With MDR, you gain a team of experienced threat hunters who vastly improve your cybersecurity 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.[2]

#3 | Is your security team overwhelmed by seemingly endless alerts?

Ideally, district teams check all of the risk alerts that EDR and other cybersecurity systems trigger.

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

If they had money to spare, districts would probably hire more cybersecurity professionals to assist. Unfortunately, the ongoing global shortage of cyber professionals leaves K-12 districts short on the financial incentives it takes to attract and maintain these highly-sought-after experts.

Is it any wonder that K-12 teams are prone to burnout—a condition otherwise known as "alert fatigue"?

> *Alert fatigue … happens to cybersecurity 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."*[xiv]

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 cybersecurity (or lack thereof) involve more than the threats themselves: K-12 districts collect and process data that is safeguarded under one or more data protection regulations, such as FERPA and CIPA.[3] Your district might need to verify compliance with data protection regulations.

Given the rising costs of protecting data and the exhorbitant costs of a breach, your district might also seek cyber insurance. If it does, you will also need a way to prove that your network cybersecurity mechanisms meet cyber insurance requirements. Failure to provide evidence of meeting those requirements might increase your premiums or preclude cyber insurance altogether.

Apart from the risk of fines for regulation violations or increased cyberinsurance premiums, as a K-12 district, your success depends on your community's trust. You might need to provide evidence to a school board (or some other community governance committee) of your efforts to protect the PII of your community's children.

> *MDR services check the compliance and regulations box …. [Services include] dashboards and reports necessary to make sure your [district] is compliant."*[xv]
>
> **–Peter Casserly**
> President, Casserly Consulting

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
- gains more time to respond appropriately to threats that matter; and
- maintain your community's trust.

ThreatDown Powered by Malwarebytes

#5 | Can you justify the expense of MDR for your district?

Your district has a fiduciary responsibility to be a good steward of public 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 cybersecurity attacks. For example, ransomware attacks increased 105% globally between 2020 and 2021, reaching a rate of nearly 20 ransomware attempts per second.[xvi]

Ransomware attacks increased 105% globally between 2020 and 2021[XVI]

Evidence of this clear and present danger should convince even the most cybersecurity 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 organizations, MDR pays for itself in approximately two months, when you factor in the cost of internal staff.[xvii]

For example, at a cost of $3 per endpoint (for 24/7/365 monitoring, investigations, triage and remediation), a school district with 1,000 endpoints would pay $3,000 per month. Now weigh that cost against the expense of hiring and maintaining inhouse cybersecurity 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.[xviii]

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

If "Yes," Then MDR Is a Sensible Option

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

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

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

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 district. Not surprisingly, MDR is growing in popularity faster than other cybersecurity options: Gartner estimates that 50% of organizations worldwide will be using MDR services by 2025.[xxi]

Given its increasing popularity, MDR might raise the bar for baseline security. If so, then not partnering with an MDR provider could leave your district 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."*[xxii]
>
> **– Peter Casserly**
> Casserly Consulting

The Ideal MDR Partner

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

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 **MRG Effitas independent lab testing results to support** results to support that claim.

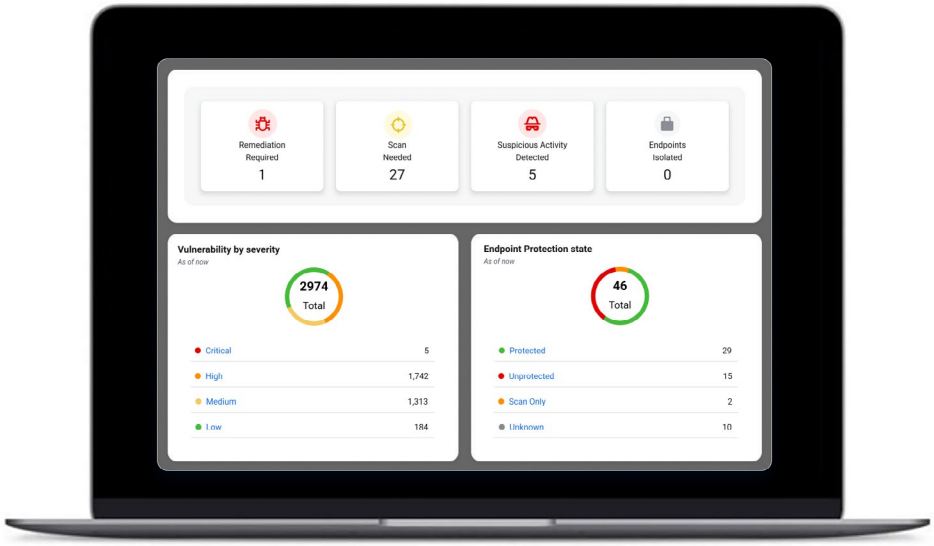
#2 The MDR team: Each MDR provider will offer different degrees of collective experience; wouldn't you like to know what you're getting? Ask. MDR analysts should be experienced cybersecurity professionals with expertise in threat detection, analysis, incident response and, ideally, data regulation requirements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

Malwarebytes' 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.

ThreatDown Powered by Malwarebytes

Introducing ThreatDown K-12 Bundle

ThreatDown K-12 Bundle is purpose-built for districts with small IT teams that lack the resources to address all security alerts and manage every student device. The ThreatDown K-12 Bundle simplifies staff and student device protection by combining award-winning technologies, including attack surface reduction, endpoint security and mobile security, with an expert managed services team to monitor and respond 24x7x365, optimizing your school's productivity and uptime as well as your security investments.



Get a free quote

ThreatDown Powered by Malwarebytes

Glossary of Cybersecurity 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 cybersecurity technology that continually scans an endpoint (e.g., laptop, PC, server) for the purpose of thwarting cyberattacks. An EDR 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: alerts that incorrectly trigger an alert indicating the presence of a cybersecurity threat, which poses a serious problem for SOC 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 cybersecurity 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 only show you 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 cyberattacks (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] Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Multi-State Information Sharing and Analysis Center (MS-ISAC), "Alert (AA22-249A): #StopRansomware: Vice Society," 6 September 2022.
[ii] S. Adam, "The State of Ransomware in Education 2021," 13 July 2021.
[iii] D. A. Levin, "The State of K-12 Cybersecurity: Year in Review—2022 Annual Report," 2022.
[iv] United States Government Accountability Office, "Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity," GAO, Washington, D.C., October 2022.
[v] See ii.
[vi] C. Page, "Hackers Leak 500GB Trove of Data Stolen During LAUSD Ransomware Attack," 3 October 2022.
[vii] A. Stone, "Early Threat Detection Helps K-12 Schools Stop Bad Actors in Their Tracks," 28 September 2022.
[viii] C. Cimpanu, "Most Ransomware Attacks Take Place During the Night or Over the Weekend," 16 May 2020.
[ix] D. Rathnayaki, "How to Deal With Cyberattacks This Holiday Season," 15 December 2022.
[x] Project Tomorrow and iboss, "Creating a Common Culture of Action Around Cybersecurity: Results from the 2021 Project Tomorrow—iboss National K-12 Education Cybersecurity Report," 2021.
[xi] See vi.
[xii] Ponemon Institute and IBM Security, "Cost of a Data Breach 2022," IBM Corporation, Armonk, NY, 2022.
[xiii] J. Oltsik, "The Growing Demand for Managed Detection and Response (MDR)," 25 April 2019.
[xiv] Techslang, "What is Alert Fatigue?" Cybersecurity Glossary.
[xv] P. Casserly, "Why Every SMB Needs Managed Detection and Response," Casserly Consulting, 2020.
[xvi] "2022 SonicWall Cyber Threat Report," 2022.
[xvii] Malwarebytes internal research.
[xviii] Malwarebytes internal research.
[xix] Malwarebytes internal research.
[xx] See ii.
[xxi] P. Shoard, C. Lawson, M. Schneider, J. Collins, M. Wah, and A. Davies, "Market Guide for Managed Detection and Response Services," Gartner Research, 2021.
[xxii] See xv.

---

[1] Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC)
[2] CISA stands for Cybersecurity and Infrastructure Security Agency, and MITRE is name of the organization that maintains the ATT&CK list, which stands for Adversarial Tactics, Techniques and Common Knowledge
[3] Family Education Rights and Privacy Act (FERPA) and Child Internet Protection Act (CIPA)