ThreatDown™
Powered by Malwarebytes

PREVENT ALL YOU CAN, MITIGATE AS YOU MUST

A Guide to Cyber Maturity for Primary and Secondary Schools

Based on a presentation by Malwarebytes Senior Solutions Engineer Robert Elworthy, this guide covers prevention and mitigation strategies that can help Primary and Secondary schools increase their cyber maturity level.

INTRODUCTION

Primary and secondary schools are under attack. In 2022, the National Grid for Learning (LGfl) and National Cyber Security Centre (NCSC) conducted an audit of cyber security in UK schools. Results indicate that 78 per cent have experienced at least one type of cyber incident. Of those, 21 per cent experienced a malware attack and 18 per cent endured "periods with no access to important information."[i]

Sadly, the situation does not appear to be improving. In fact, Malwarebytes Labs recently determined that the UK education sector currently suffers a disproportionately high percentage of ransomware attacks: Between April 2022 and March 2023, the education sector claimed 16 per cent of known ransomware attacks in the UK,[1] making it the second most targeted industry after services (at 27 per cent).[ii]

Ransomware and other attacks can leave schools with little choice but to cancel classes whilst an overworked IT team scrambles to bring operations back online. Attacks may also result in ransom demands of tens of thousands—if not millions.

Further, anyone whose personal identifiable information (PII) is compromised may be eligible to claim data breach compensation from the breached school.[2]

- September 2023 brought a spate of attacks against UK schools. Highgate Wood School in Crouch End, managed to escape the worst results of attack but left parents of its 1500 pupils scrambling to find childcare after delaying its start time by nearly a week.[iii]
- In January 2023, attackers demanded £15 million in ransom from at least 16 secondary schools hit over the Christmas holidays. The attacks delayed start times and shut down email access, costing countless students work placements and university interviews.[iv]
- When a cyber criminal group demanded nearly £3 million from the Harris Federation, it refused. After more than 10 days of negotiations and a ransom that attackers doubled then reverted, the Federation held firm to their refusal, and attackers retaliated by releasing confidential data of the academy chain's 38,000 pupils.[v]

Stolen PII: What's the Big Deal?

When cyber criminals steal PII, they often post it on the dark web. The "dark web" uses internet infrastructure but operates privately; to access it, criminals use specific configurations and authorization methods.

Criminals can use stolen PII to:

- open (or use an existing) credit card or bank account
- apply for (and default on) loans
- create an online account (e.g., retirement, health spending)—or use an existing one

In 2023, PII, passport scans, and staff pay scales from 14 UK schools were leaked by the ransomware group Vice Society.

[1] Malwarebytes Labs does not include attacks for which victims paid the ransom in their tally of "known" attacks.
[2] PII is any data that when used alone or with other data that can identify an individual, such as a National Insurance Number, Special Education Needs (SEN), immigrant status, gender, race, or birthdate.

A SECURITY PLAN: WHY NOT START TODAY?

Despite the risk and cost of a breach, our schools remain underprepared for cyber-attack. One in ten primary schools have taken no steps to mitigate the aftermath of an attack.[vi]

The education annex to the government's "Cyber security breaches survey 2023" also speaks to our schools' lack of awareness regarding cyber security.[vii]

Among a handful of other questions, the survey asked respondents to indicate whether or not they were aware of these (and other) government sources:

- The 10 Steps to Cyber Security guide, which summarises what organizations should do to guard against successful cyber attacks
- The government-endorsed Cyber Essentials scheme, which encourages organisations to seek independent certification to verify they have met a set of five "essential" cyber security practices
- The NCSC's Board Toolkit, which "helps boards to ensure that cyber resilience and risk management are embedded throughout an organization"[viii]

In sum, these sources are all designed to help organisations strengthen their cyber security practices. Hence, it stands to reason that to be assured of alignment with good-practice standards, organisations must first be *aware* of the sources that outline those standards.

Unfortunately, the government survey reveals that primary and secondary schools have limited awareness of these and other government cyber security initiatives: A mean average of only ~34 per cent of schools answered these questions in the affirmative. (See Figure 1.) Furthermore, nearly half of the schools surveyed (47 per cent) confessed that they do not feel prepared for an attack.[ix]

Barring awareness of these guidelines and implementation of all recommended practices, your school can improve its cyber security posture—and you can start today. This guide covers five topics designed to help you determine where to focus your efforts and dollars to increase your institution's fortifications:

1. Risk assessment
2. Backup strategy
3. Training
4. Prevention
5. Mitigation

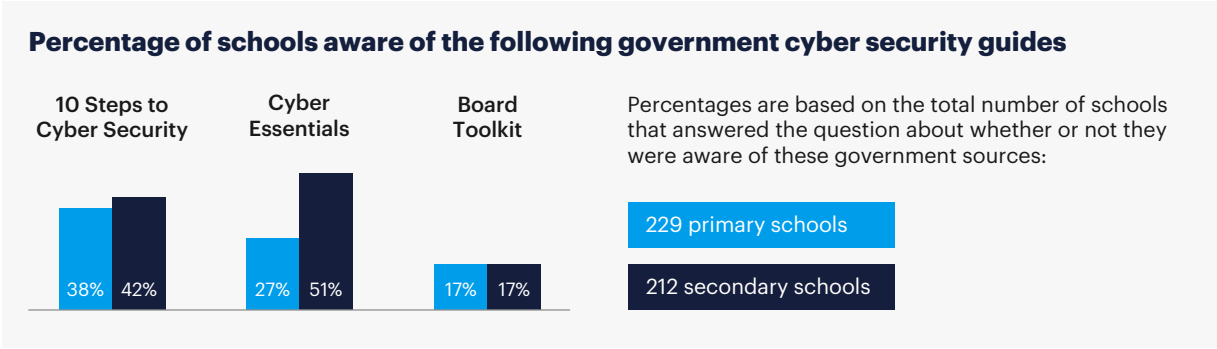

Figure 1. Primary and secondary schools lack awareness of the government-endorsed sources designed to help organisations strengthen their cyber security practices.

WHAT'S IN IT FOR YOU?

The end goal is to create, implement, test, verify and routinely review a solid cyber security plan—a document defining your institution's cyber security policies, procedures, strategies, and technologies. (See Figure 2.)

The plan will describe the steps your institution takes to:

- Prevent as many cyber-attacks as possible
- Mitigate cyber incidents at minimal cost

A plan for mitigation is as essential as a plan for prevention: Regardless of the number and strength of your defense measures, cyber criminals never give up. **You must adopt a mindset of not only, "What can we do to avoid an incident?" but also, "What will we do *when* we experience one?"**

A cybersecurity plan will help your institution:

- Implement cyber security frameworks (e.g., Cyber Essentials and Cyber Essentials Plus)
- Comply with regulations (e.g., EU General Data Protection Regulation and UK Data Protection Act)
- Gain or maintain cyber insurance
- Respond swiftly and effectively to incidents to:
  - minimise disruptions to learning
  - responsibly manage funds
  - preserve users' privacy and confidential data
  - maintain the community's trust

ASSET	THREAT	VULN	IMPACT	ODDS	SEVERITY	ACTION
CRITICAL **Servers**	CRITICAL External threat actor breaches data store with PII	HIGH Firewall in place; server runs EDR*; manual patching process	CRITICAL Student, staff, faculty PII exposure	HIGH PII currently unencrypted; backups and OS patching process irregular	HIGH Potential loss of $$, time and community trust	Encrypt data; automate daily backups (encrypted); automate vulnerability scanning and patching process
MEDIUM **Website**	HIGH Malicious human (internal or external)–DDOS attack	MEDIUM Firewall properly configured; server running EDR	MEDIUM Website resources temporarily unavailable	LOW Have experienced only one DDOS attack in 2 years	LOW Frustrated students and parents	Continue monitoring firewall and EDR activity

Figure 2. The risk assessment report you create can take any form. This is only one example.

* Endpoint Detection and Response (EDR)

STOP: CONSIDER THE STAKES

Assess your institution's risk profile to steer your plan

To begin formulating a cyber security strategy, the first step is to conduct a risk assessment. A risk assessment makes plain which assets you are defending and from what.

In cyber security, "risk" is commonly represented as an equation.

RISK = THREAT x VULNERABILITY x IMPACT

Despite its appearance, this "equation" is not a mathematical formula but rather a model. The model demonstrates "risk" as being determined by a combination of factors, namely threat, vulnerability, and impact (or cost). When identifying risks, you must also assess the likelihood that the vulnerabilities you identify will allow a threat to occur.[x]

- **Threat is any event that could harm your institution's assets or users** (e.g., students, staff, and teachers). Cyber incidents, website failures, and natural disasters are examples of threats.
- **Vulnerability is any potential weak point that could allow a threat to cause damage.** Outdated or unpatched software is a vulnerability; such software has known bugs that attackers can exploit to gain network access. If your server room is located in a basement, that location might be a vulnerability; this location might increase the likelihood of water (from a flood or hurricane) damaging your servers.
- **Likelihood is the probability that a threat will occur.** Determining likelihood is implicit in uncovering vulnerabilities. For example, if you do not scan your endpoints for Common Vulnerabilities and Exposures (CVEs), then the likelihood that an attacker will exploit a Windows CVE is very high

As this example illustrates, likelihood defines the degree of risk (e.g., High, Medium, Low).

- **Impact is the aftermath of a threat that has become an incident (i.e., caused harm).** For example, suppose the OS on most of your servers has a patch available for a CVE but you and your team have not yet found the time to test and apply the patch.

Meanwhile, a cyber criminal organisation finds the vulnerability, uses it to gain access to your network and, days or weeks later, launches a ransomware attack and succeeds in encrypting (or stealing and threatening to post) sensitive data.

The impact, in this case, might include institution-wide school closures, recovery costs, and the public exposure of PII.

STOP: CONSIDER THE STAKES

Where and how to start

To help you begin the process of identifying your institution's risk profile, consider these five assessment goals and corresponding questions:

For more information about risk assessments, read this article from Malwarebytes Labs.

	ASSESS	QUESTION
1	**Assets**	**What and where are our assets?** *(Make a complete list of your servers, applications, and data.)*
2	**Threats**	**What events could harm our assets?**
3	**Vulnerabilities**	**What are weak points in our systems that could allow a threat to cause damage?**
4	**Impact/Probability**	**What is the cost associated with the threat and how likely is it to occur?** *(Consider using color-coded words to indicate the likelihood of each threat and vulnerability: **HIGH**, **MEDIUM**, **LOW**)*
5	**Relative importance of assets**	**If this asset were lost or exposed, what would be the degree of impact?** *(Consider using color-coded words to indicate the importance of each asset: **CRITICAL**, **HIGH**, **MEDIUM**, **LOW**)*

3 – 2 – 1: START YOUR DEFENSES

Create foolproof backups for baseline protection

Suppose your team arrives one morning only to find a ransomware note flashing across all server and workstation monitors. Now assume that the note reveals that attackers have encrypted all your critical data. You can restore it, the note claims, by paying the ransom.

Suddenly, NOT paying might seem reckless—particularly if you do not have ready access to clean backups that escaped the attackers' notice.

Of course, the UK government and cyber security industry leaders advise against paying the ransom. The NCSC plainly states that, "Law enforcement do not encourage, endorse, nor condone the payment of ransom demands." By paying a ransom you fund criminals. Furthermore, the NCSC claims, paying leaves you, "more likely to be targeted in the future."[xi]

When your systems are inaccessible, however, you might not care about these hypotheticals—but there is another reason you should not pay: Paying does not guarantee that you will be able to restore your data. For example, the NCSC guidelines note that some malware, for example, wiper malware, may *present* as ransomware but prohibit data recovery whether or not you pay the ransom.

To prepare for the possibility of a ransomware attack and gear up for answering "No" to the ransom demand, you need to feel confident about your backups.

Backups are critical to data protection, and the **3-2-1 backup strategy is widely recognized as a best practice**. (See Figure 3.)

Figure 3. The 3-2-1 backup strategy: 3 copies on 2 storage media with 1 off-site.

3	**Keep THREE COPIES**	To ensure that you can always recover your data, keep three copies. In practice, this usually means having one primary copy that is easily accessible and two additional copies that serve as backups.
2	**Store copies on TWO DIFFERENT MEDIA**	Storing all data on the same storage media increases the likelihood of losing access because all same-type storage devices could fail. To avoid this, store your data on at least two different types of storage media, such as hard drives, tape drives, and the cloud.
1	**Store at least ONE COPY OFFSITE**	Storing all data in the same location leaves it vulnerable to data loss from a natural disaster. To foolproof your backup strategy, store at least one copy of all data in a location that is off-site.

3 – 2 – 1: START YOUR DEFENSES

Data recovery (easy as 1-2-3)

Implementing a 3-2-1 backup strategy cannot guarantee that *all* of your data can *never* be compromised. However, it does eliminate the risk of a single point of failure. In the event of an attack or other catastrophic event, if you have implemented the 3-2-1 backup strategy, you will likely have the means to restore your data.

Consider this hypothetical scenario in which your institution is attacked:

- **Production copy is encrypted**. When you see the note, you pull out your laptop or any other machine that was disconnected when the attack occurred. You connect your storage media directly to your laptop to check the integrity of your backups.
- **Second copy unusable**. Suppose you find that the hard disk drive you used to back up your production data has also been encrypted, and your tape copy is damaged.
- **Off-site copy to the rescue**. In this case, only your off-site backup is usable so that is the data you must restore.

The challenge, of course, is maintaining *current* backups, so you need to research your options for a backup solution carefully. **The more frequently you back up your data, the more current it will be when you restore it; and the easier you make backing up your data, the more frequently you will do so.**

For more information on the 3-2-1 backup strategy, see articles from Malwarebytes Labs here and here.

TRAIN YOUR USERS: DON'T GET SCHOOLED

Engage students, staff, and faculty in cybersecurity training

No matter how advanced, technology alone cannot prevent a student (or employee or professor) from clicking a link in an email that appears legitimate. In education, the odds of a user falling for such an attack are stacked against you: **76 per cent of breaches in education are attributable to what the Verizon Data Breach Investigations Report refers to as "the human element."**[xii]

To err is human. We all know it; cyber security just underscores it. In fact, research suggests that "users continue to be the most significant flaw in organizations' cyber defense layer."[xiii]

The answer? Training. Training is key to offsetting the trusting nature of humans and to minimising the mistakes they make that jeopardise your network. Whilst no amount of training can prevent all attacks, effective cyber security training can reduce their rate. And yet, 45 per cent of schools do not train non-IT staff about cyber security.[xiv]

That said, primary and secondary schools face a number of challenges when it comes to cyber security training, not the least of which are tight budgets and limited time. So, let's begin by addressing the potential elephant in the room: Does cyber security training actually help?

Training makes a difference

A 2020 analysis by USENIX Association answers the question: Yes, training helps—quite a lot. USENIX researchers held cyber security training for approximately 410 employees of a German government organisation. USENIX focused its research on the workers' response to phishing training.[xv]

Prior to and immediately after training, the researchers conducted a test. Immediately after training, the employees were significantly better at detecting phishing messages: **80 per cent correctly identified phishing messages after training compared to only 62 per cent before.**

Researchers also found that the effects of training wear off. **Consequently, researchers recommend reaffirming training messages every six months.** Furthermore, this study showed that re-training using video was the most effective (followed by interactive examples.)

Training can yield equally promising results in a primary or secondary school.

A 2023 KnowBe4 benchmarking report on phishing analysed data from more than 12.5 million users among 35,681 organisations across 19 different industries worldwide, including education. Prior to training users on recognising phishing attacks, KnowBe4 researchers established a baseline for what they call the "Phish-prone™ Percentage (PPP)," which represents users' susceptibility to phishing attacks.[xvi]

TRAIN YOUR USERS: DON'T GET SCHOOLED

Pre-training, the average PPP score for the education industry ranged from 30.3 per cent (for populations >1000) and 31.2 per cent (for populations <250). After 90 days of training, education institutions improved their PPP score by up to 41 per cent. **After one year of training, the results were even more dramatic, with PPP scores in education improving by as much as 85 per cent.** For example, institutions with fewer than 250 users dropped from a PPP of 31.2 per cent to only 4.6 per cent.

Getting started

To help you create a vision board for what your training efforts might look like—not to mention the results they could yield—consider these four suggestions:

1	**Phishing: Third-party help**	Use a third-party solution to borrow ready-made educational content and conduct periodic phishing simulations. (Examples of third-party providers of such solutions include KnowBe4, Infosec IQ, Proofpoint, and Mimecast.)
2	**Phishing: In-house training**	Create your own brief email, video or interactive simulation to train your users how to recognize phishing messages. Conducting in-house training might be as simple as identifying which end users are most likely to open phishing emails and communicating directly—and empathetically—with them.
3	**Distributing materials: Creative options**	Why not write and distribute an institution-wide email about cybersecurity—one that's both informative and fun? What about a monthly (or bi-monthly) newsletter? How about a webinar?
4	**Building relationships: Users and IT**	The safer students, staff and faculty feel about approaching IT with questions or concerns about cybersecurity, the more apt they are to do so. Create a welcoming environment so that your institution's users feel comfortable communicating with your team.

For more information about training students, staff, and teachers on cyber security matters, visit the NCSC "Education & skills" web page.

DEFENSE-IN-DEPTH: THE BEST ANSWER TO PREVENTION

Deploy layers of preventative measures

Nearly 70 per cent of all breaches originate at endpoints,[xvii] which speaks to the need to secure them—but what technology does the job best?

The most advanced technology for endpoint protection available today is Endpoint Detection and Response (EDR). In today's world of organised cyber crime, endpoint solutions that offer prevention-only capabilities (such as old-school antivirus products) are not enough. EDR offers both preventative and mitigative capabilities.

In terms of preventative capabilities, EDR delivers layers of measures for defense-in-depth. **As Malwarebytes Senior Solutions Engineer Robert Elworthy explains, "defense-in-depth has been and remains the best answer" to prevention.**

An EDR stack should provide at least these preventative capabilities:

	CAPABILITY	WHAT TO LOOK FOR
1	**Anti-Malware**	Use a solution that leverages "real-time protection," a feature that prevents malware, such as ransomware, from being installed on devices in your IT environment.
2	**Anti-Exploit**	Use a solution that leverages an anti-exploit feature to prevent attackers from delivering malicious payloads using known software vulnerabilities.
3	**Device Control**	Use a solution that leverages device control. Device control reduces the risk of data loss and theft by managing and blocking unauthorised USB devices and removable storage media from connecting to your institution's network.
4	**Vulnerability Assessment**	Use a solution that allows you to scan your IT environment on demand or as scheduled. Scanning can uncover CVEs in applications, operating systems, and drivers across your cross-platform endpoint fleet.
5	**Patch Management**	Use a solution that can automate the patching process to minimise the time between when a patch is available and when it is applied. Minimising this timeframe reduces the risk of an attacker exploiting known vulnerabilities. (Up to 60 per cent of breaches could be avoided by applying available patches.)[xviii]
6	**DNS Filtering**	Use a solution that leverages DNS Filtering, a feature that automatically blocks traffic originating from known malicious domains, URLs, and IP addresses.

RESPOND AND RECOVER: YOUR PLAN FOR MITIGATION

Minimise impact with the right strategy, processes, and tools

Sadly, no matter how many layers of sophisticated preventative measures you deploy on network endpoints, persistent cyber criminals will find ways to sneak onto your network.

This is where EDR shines: An EDR solution is designed to detect, analyse and respond to the obfuscated threats that manage to slink past all initial lines of defense.

EDR solutions conduct three critical tasks:

- collect data from endpoints in real time
- use that data to establish "normal" patterns of user and application behaviour
- apply data analysis techniques that detect unusual patterns of behaviour to uncover hidden (and as-yet unknown) threats lurking on your network

When it detects threats, an EDR solution's "response" capabilities come into play. Look for a solution that makes it easier for you to manage the threats it detects by offering these capabilities:

	CAPABILITY	WHAT TO LOOK FOR
1	**Contextual detections**	EDR solutions alert you of detected threats. Choose a solution that allows you to select the delivery method (e.g., email or a messaging app, such as Slack). More importantly, look for a solution that offers "contextual" detections. Contextual detections include enough information for you to understand what happened, where it happened, and what you're supposed to do about it.
2	**Automated containment**	An EDR solution can automatically "quarantine" (that is, isolate) processes, subnets, and endpoints when it detects certain threats to prevent further spread across your network.
3	**One-click remediation**	An EDR solution can automate remediation whilst also allowing for manual remediation. Use a solution that enables you to *easily* remediate or restore quarantined threats.
4	**Rollback**	Use a solution that includes a rollback feature. EDR solutions with this feature periodically capture images of endpoints. These captured images allow you to re-image an endpoint—or roll it back—to restore it to a good state in the event of an attack. A rollback feature should allow you to thus restore an endpoint—without relying on Microsoft's Volume Shadow Copy Service (VSS). (Some ransomware groups, such as Conti, locate and delete shadow copies that VSS creates.)
5	**Analytic coverage for proactive threat hunting**	An EDR solution functions like a flight data recorder for your endpoints. During a flight, an airplane's black box records dozens of data points (e.g., altitude, air speed, and fuel consumption). In the aftermath of a plane crash, investigators use the data from the black box to determine what factors may have contributed to the plane crash. These factors are then used to prevent similar crashes in the future. Likewise, an EDR solution collects endpoint telemetry before, during, and after an attack (e.g., active processes, installed programmes, and network connections). The best EDR solutions provide the highest level of detail available. Cyber security experts use the data EDR collects to conduct threat hunting, proactively searching for signs of threats to stop them before they cause harm.

RESPOND AND RECOVER: YOUR PLAN FOR MITIGATION

Where MDR comes into play

Whilst EDR is the most advanced software technology for endpoint security available today, EDR alone has limitations. For example, EDR can gather information and deliver the highest degree of analytic coverage, but it takes human experts to scour those logs. Unfortunately, EDR alerts are too often ignored. According to IDC, IT teams ignore or do not investigate as many as 30 per cent of EDR alerts.[xix]

In primary and secondary schools, this percentage would likely be as poor (if not poorer) due to limited resources. Budgets are always tight for schools, which perhaps explains the limited training amongst IT staff. According to RM research, 56 per cent of primaries and 43 per cent of secondaries state that those responsible for cyber security receive training less than once yearly—and 18 per cent of primaries receive no training at all.[xx]

As Malwarebytes cyber security expert Matt Sherman explains, "Software stops software; people stop people."

This is where Managed Detection and Response (MDR) solutions step in. MDR solutions are built on an EDR technology stack that a remote team of the vendor's cyber security experts continually monitors 24/7/365.

An MDR team of cyber security experts does not supplant your inhouse team. It augments your team, helping you stay apace of EDR alerts and proactively threat hunt. This can be particularly useful to primary and secondary schools, which commonly have small (typically overworked) IT teams that might have skills gaps that preclude effective threat hunting.

THREATDOWN MEETS HIGHER EDUCATION NEEDS

Detect earlier, respond faster with ThreatDown EDR

ThreatDown, powered by Malwarebytes, is committed to partnering with primary and secondary schools to ensure the protection of students, staff, teachers, and data. Education organisations around the world, including schools like yours, are turning to ThreatDown, powered by Malwarebytes, cyber security solutions because:

- ThreatDown, powered by Malwarebytes, solutions deliver the preventative and mitigative capabilities schools need
- ThreatDown, powered by Malwarebytes, solutions are purpose-built for resource-constrained teams

ThreatDown EDR is award-winning technology that delivers effective protection—from prevention through detection to mitigation—that teams with emerging cyber security acumen can learn and use with ease.

Its simplicity belies its underlying sophistication: ThreatDown EDR includes high-powered tools and customisable options that users can embrace as their skills levels grow and their schools' needs change.

By deploying our readily accessible cloud-based security platform, your organisation will gain powerful detection and remediation capabilities, whilst freeing your team to spend time on other more pressing projects. ThreatDown EDR promises:

- **Accelerated deployment across your diverse endpoint fleet**: We designed ThreatDown EDR with ease in mind to simplify and accelerate deployment; our lightweight agent deploys within hours. We offer endpoint security for every platform: Windows and Mac workstations, Windows and Linux servers, iPads, Chromebooks, and even Android and iOS phones.
- **Ease of management**: Powerful protection managed by way of our easy-to-use cloud-based Nebula console for managing *all* of your endpoints from a single location. Our intuitive dashboard displays visual cues to immediately convey which endpoints need attention and why. Manage your endpoints from anywhere you have internet access and a Chrome browser—from your workstation, laptop, or even iPhone.
- **Defense-in-depth prevention**: Anti-malware, anti-exploit and defense control are built in. Activate our Vulnerability Assessment, Patch Management, and DNS Filtering

THREATDOWN MEETS HIGHER EDUCATION NEEDS

modules with a few clicks from within the Nebula console.

- **Contextualised detections without the noise**: Detected threats trigger alerts that contain information that helps you quickly make informed decisions about how to respond appropriately. Our EDR delivers precise threat detection with few (if any) False Positives.
- **Expanded remediation**: With a few clicks from within our cloud-based management console, you can remotely remediate an infected endpoint. Our industry-renowned, proprietary Linking Engine is designed to identify and remove residual malware-related artifacts and infection-induced changes for thorough remediation.

Uplevel your endpoint security with ThreatDown MDR

IT teams at primary and secondary schools commonly have limited staff and resources and consequently struggle to manage protection across hundreds and sometimes thousands of cross-platform endpoints. If this is true of your schools, your team would likely benefit from managed endpoint security services.

Built on our award-winning EDR technology stack, ThreatDown MDR provides powerful threat detection and remediation services. Using threat intelligence from internal and external sources, ThreatDown MDR delivers the following: 24/7/365 monitoring, threat prevention and detection; patent-pending active campaign threat hunting and human-led proactive threat hunting; rapid alert notification; and incident response (including triage and remediation). At a price point within reach, ThreatDown MDR empowers your school to maximize its cyber security posture and resilience.

ThreatDown MDR is a force multiplier for your security operations. Our elite team of security experts effectively closes your security resources gap, reduces your risk of unknown threats, and increases your security efficiency exponentially.

We offer two levels of managed services: Managed Threat Hunting (MTH) and MDR. Feel free to contact us to discuss which of these options would best suit your institution's needs.

For more information about ThreatDown MDR, see this post from Malwarebytes Labs; for information about our MTH service, visit our web page on the subject.

LEARN MORE

Contact us today to learn more about how ThreatDown, powered by Malwarebytes, can help you prevent all you can while mitigating what you must.

Try now >

[i] National Cyber Security Centre (NCSC) and National Grid for Learning (LGfl). (2022.) "Cyber Security Schools Audit 2022."
[ii] Malwarebytes Labs. (April 2023.) "Ransomware in the UK, April 2022 – March 2023."
[iii] Muncaster, Phil. (5 September 2023.) "More Schools hit by Cyber-Attacks Before Term Begins." *InfoSecurity Magazine.*
[iv] Lodge, Matthew. (6 January 2023.) "Hacky new year!" *DailyMail.*
[v] Podcast. (13 July 2021.) "Held to Ransom." File on 4.
[vi] RM. (3 October 2022.) "Half of schools' cyber security experts receive little or no training annually, despite the education sector being at most risk of cyber threats."
[vii] Gov.UK. (19 April 2023.) "Cyber security breaches survey 2023: education institutions annex."
[viii] NCSC. "Cyber Security Toolkit for Boards." Accessed 12 September 2023.
[ix] NCSC and LGfl. (2022.) "Cybersecurity in schools—are we teaching and learning? Analysis and next steps from the 2022 audit of cybersecurity in UK schools."
[x] Sotnikov, Ilia. (2018.) "How to Perform IT Risk Assessment." Netwrix.
[xi] NCSE Guidance. "Mitigating malware and ransomware attacks."
[xii] Verizon 2023 Data Breach Investigations Report.
[xiii] Collard, Anna et al. (2023). "Phishing by Industry Benchmarking Report: 2023 Edition." KnowBe4.
[xiv] See ix.
[xv] Reinheimer, Benjamin et al. (2020.) "An Investigation of Phishing Awareness and Education over Time: When and How to Best Remind Users." USENIX.
[xvi] Collard, Anna et al. (2023). "Phishing by Industry Benchmarking Report: 2023 Edition." KnowBe4.
[xvii] Bridgehead IT. "Best Practices for Endpoint Detection and Response."
[xviii] ServiceNow. (2020.) "Costs and Consequences of Gaps in Vulnerability Response." Ponemon Institute.
[xix] Robinson, Craig. (October 2021.) "In Cybersecurity, Every Alert Matters." IDC.
[xx] See vi.

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