eBook

ThreatDown™
Powered by Malwarebytes

K-12 Guide to Cybersecurity

Prevent what you can, mitigate what you must

Introduction

Over the last six years, the nation's schools have disclosed an average of more than one cyber incident[1] per school day—and that's not the whole story. The actual rate of K-12 cyber incidents is likely worse: Estimates suggest that the real rate (including undisclosed incidents) is 10 to 20 times higher.[i]

The types of cyber incidents US schools face vary, but the most frequently disclosed involve ransomware, which aligns with the global attack trend. In January 2023 alone, Malwarebytes Labs detected 21 ransomware attacks targeting the global education sector, placing **education as the second most targeted industry worldwide**.[ii]

Ransomware attacks disrupt learning, take a toll on already-tight school budgets, and too often expose student, staff and faculty personal identifiable information (PII):[2]

- A January 2023 ransomware attack on four public schools serving 1,700 students in Nantucket, Massachusetts shut down all student and staff devices, forcing the schools to close.[iii]
- The impact of a cyberattack on schools can lead to a loss of learning time ranging from three days to three weeks and recovery from these attacks can take anywhere from two to nine months, costing schools between $50,000 and $1 million per cyberattack.[iv]
- In September 2022, the second largest district in the country suffered a ransomware attack that was later widely publicized. When Los Angeles Unified School District refused to pay the ransom, the attackers posted 500GB of district users' PII.

Stolen PII: What's the big deal?

When cybercriminals steal student, staff and faculty PII, they often post it on the dark web. (The "dark web" uses internet infrastructure but operates privately; to access it, criminals use specific software configurations and authorization methods.)

Criminals can use stolen PII to:

- Open a credit card or bank account—or use an existing one
- Apply for (and default on) loans
- Create an online account (e.g., retirement, health spending)—or use an existing one

Student PII is especially valuable because kids don't track their credit scores, so a criminal can potentially abuse the stolen info for decades without anyone noticing.

[1] A cyberattack is considered an "incident" when a threat actor gains unauthorized access to IT systems, actually or potentially compromising those systems or the information the systems hold.

[2] PII is any data that when used alone or with other data can identify an individual, such as a Social Security number, immigrant status, gender, race, or birthdate.

A Security Plan: Why Not Start Today?

Despite the evident risk and potential cost of a breach, K-12 districts remain underprepared for cyberattacks, as indicated by their low cyber maturity ranking.

The K-12 sector averaged a cyber maturity score of 3.55 on the Nationwide Cybersecurity Review (NCSR) scale. The NCSR ranks organizations' security programs on a scale of 1 through 7, where a "1" is the lowest maturity (and consequently the highest risk). **With a 3.55 score, the K-12 sector falls short of the recommended minimum maturity level of 5**.[v] (See Figure 1.)

You can start today to improve your district's cyber maturity score. This guide intends to help you better understand five topics to explore and act upon to help you determine where to focus your efforts and dollars to increase fortifications:

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

Score	Maturity Level	Description
7	**Optimized**	Your district has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified**	Your district has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process**	Your district has formally documented policies, standards, and procedures and is in the process of implementation.
4	**Partially Documented Standards and/or Procedures**	Your district has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy**	Your district has a formal policy in place.
2	**Informally Performed**	Activities and processes may be substantially performed and technolgies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed**	Activities, processes, and technolgies are not in place to achieve the referenced objective.

***Figure 1**: The NCSR uses a maturity scale to assess how organizations are addressing cybersecurity. The recommended minimum maturity level is a 5; K-12 organizations average a score of 3.55.*

ThreatDown™ Powered by Malwarebytes

What's in It for You?

The end goal is to create, implement, test, verify, and routinely review a solid cybersecurity plan—a document defining your district's cybersecurity policies, procedures, strategies, and technologies. (See Figure 2.) The plan will describe the steps your district takes to:

- prevent as many cyberattacks as possible
- mitigate cyber incidents at minimal cost

A plan for mitigation is as essential as a plan for prevention because regardless of the number and strength of your defense measures, cybercriminals 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 district:

- comply with data regulations (such as FERPA)
- gain and maintain cyber insurance
- respond swiftly and effectively to incidents (such as ransomware) to:
  - minimize disruptions to learning
  - responsibly manage taxpayer dollars
  - preserve your users' privacy and confidential data
  - maintain your community's trust

Asset	Threat	Vulnerability	Impact	Odds	Severity	Action
Servers **CRITICAL**	External threat actor breaches data store with PII **CRITICAL**	Firewall in place; server runs EDR*; manual patching process **HIGH**	Studen, staff, faculty PII exposure **CRITICAL**	PII currently unencrypted; backups and OS patching process irregular **HIGH**	Potential loss of $$, time and community trust **HIGH**	Encrypt data; automate daily backups (encrypted); automate vulnerability scanning and patching process
Website **MEDIUM**	Malicious human (internal or external)—DDOS attack **HIGH**	Firewall properly configured; server running EDR **MEDIUM**	Website resources temporarily unavailable **MEDIUM**	Have experienced only one DDOS attack in 2 years **LOW**	Frustrated students and parents **LOW**	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 district's risk profile to steer your plan

To begin formulating a cybersecurity strategy, the first step is to conduct a risk assessment. A risk assessment will help you better understand what you are defending and from what.

In cybersecurity, "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.[vi]

- **Threat is any event that could harm your district's assets or users** (i.e., students, faculty, staff, or potentially even parents).

  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.**

  Vulnerabilities come in all shapes and sizes. For example, outdated or unpatched software have known bugs that attackers commonly exploit to gain access to a network.

  If your server room is located in a basement, that location might be a vulnerability; it 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 had a patch available for a CVE but you and your team had not yet found the time to test and apply the patch.

  Meanwhile, a cybercriminal organization finds the vulnerability, uses it to gain access to your network and, days or weeks later, launches a ransomware attack and succeeds in encrypting your district's data.

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

Where and how to start

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

Access	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:* ***HIGH****,* ***MEDIUM****,* ***LOW****)*

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

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, US government agencies and cybersecurity industry leaders advise against paying the ransom, in part because paying rewards the bad guys. As the FBI points out, rewarding attackers might encourage them "to target more victims" and inspire other budding cybercriminals to give ransomware a shot.[vii]

When your school doors are closed, possibly districtwide, 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**.

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.

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 district 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 also 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 teachers in cybersecurity training

In a recent survey, ThreatDown, powered by Malwarebytes, found that very few schools (16%) require cybersecurity training for students, teachers, or staff that connect to the school network.[vii] Given that the survey was conducted at the height of the pandemic (when distance learning was the new normal), the finding (while arguably not surprising) is disturbing.

Technology alone—no matter how advanced and sophisticated—cannot save you from a naïve and uninformed staff member falling for a phishing scheme. Training is key to offsetting the trusting nature of humans and to minimizing the mistakes they make that jeopardize your network. While no amount of training can prevent all attacks, effective cybersecurity training can reduce the rate of attacks.

For example, suppose you focused your training efforts on passwords and phishing. Discounting errors that lead to a minority of breaches, the two most common routes that attackers take to gain network access involve credentials (~50%) and phishing (~20%).[ix]

How many threats could you potentially thwart by training users on the importance of creating strong passwords and not sharing them?

How many more could you prevent by training them NOT to click links from emails they weren't expecting?

Training makes a difference

K-12 districts face a number of challenges when it comes to cybersecurity 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 cybersecurity training actually help?

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

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

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.)[xii]

Training can yield equally promising results in a K-12 environment.

West Aurora Public School District 129 serves five Illinois counties with 12,500 students and 1,500 staff. District 129 had invested in the right preventative technologies, but not in training. Two events inspired training efforts: First, the district suffered a two-month span of weekly DDoS attacks. Second, a neighboring district fell victim to a phishing attack, which resulted in the exposure of staff PII.

District 129 decided to ramp up end-user training on security in general and phishing in particular. Over the course of five months, the district focused on training staff and teachers to be more aware of cybersecurity hazards. **The results of training were dramatic: In five months, this K-12 district's monthly phishing rates dropped from 27% to .03%**.[xiii]

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 a district-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 teachers 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 district users feel comfortable communicating with your team.

ThreatDown™ Powered by Malwarebytes

Defense-in-Depth: The Best Answer to Prevention

Deploy layers of preventative measures

Nearly 70% of all breaches originate at endpoints,[xiv] 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 bundled in solutions built on Endpoint Detection and Response (EDR). In today's world of organized cybercrime, 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 **Next-Gen Antivirus**	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 unauthorized USB devices and removable storage media from connecting to your district'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 minimize the time between when a patch is available and when it is applied. Minimizing this timeframe reduces the risk of an attacker exploiting known vulnerabilities. (Up to 60% of breaches could be avoided by applying available patches.)[xv]
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.

ThreatDown™ Powered by Malwarebytes

Respond and Recover: Your Plan for Mitigation

Minimize impact with the right strategy, processes, and tools

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

This is where EDR shines: An EDR solution is designed to detect, analyze 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 behavior
- apply data analysis techniques that detect unusual patterns of behavior 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" (or 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 while 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 programs, and network connections). The best EDR solutions provide the highest level of detail available. Cybersecurity experts use the data EDR collects to conduct threat hunting, proactively searching for signs of threats to stop them before they cause harm.

Where MDR comes into play

While EDR is the most advanced software technology for endpoint protection 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.

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 cybersecurity experts continually monitors 24x7x365.

An MDR team of cybersecurity experts does not supplant your inhouse team. It augments your team, helping you stay apace of the alerts that EDR generates and proactively threat hunt. This can be particularly useful to school districts, which typically have small (often overworked) IT teams that might have skills gaps that preclude effective threat hunting.

> *Software stops software; people stop people."*
>
> **–Matt Sherman**
> MDR Expert, Malwarebytes

ThreatDown, powered by Malwarebytes, meets K-12 needs

Detect earlier, respond faster with ThreatDown K-12 Bundle

ThreatDown, powered by Malwarebytes, is committed to partnering with districts and schools to ensure the protection of students, faculty, staff, and data. Education organizations around the world, including school districts like yours, are turning to ThreatDown, powered by Malwarebytes, cybersecurity solutions because:

- ThreatDown solutions deliver the preventative and mitigative capabilities school districts need
- ThreatDown solutions are purpose-built for resource-constrained teams

> *Malwarebytes' results underscore the effectiveness and importance of leveraging machine-learning driven processes to combat novel forms of malware and prevent false positives."*
>
> **–MRG Effitas**

ThreatDown K-12 Bundle is award-winning technology that delivers effective protection—from prevention through detection to mitigation—that teams with emerging cybersecurity acumen can learn and use with ease.

Its simplicity belies its underlying sophistication: ThreatDown K-12 Bundle includes high-powered tools and customizable options that users can embrace as their skill level grows and their district's needs change.

You don't have to take our word for it

We have the third-party evaluation results to support our claims; we encourage you to review them and to compare our results against the results of our competitors. (Learn more in this Endpoint Security Evaluation Guide.)

MRG Effitas Q4 Results

- Malwarebytes scored a **perfect 100%** across all test categories with **ZERO False Positives**.
- Malwarebytes is the **ONLY** vendor to earn 37/37 award certifications and logos since Q3 2021.
- In Q3 2023, Malwarebytes was awarded the **new Phishing certification** by automatically blocking all in the wild phishing test cases.

Detect earlier, respond faster with ThreatDown K-12 Bundle

By deploying our readily accessible cloud-based security platform, your district will gain powerful detection and remediation capabilities, while freeing your team to spend time on other more pressing projects. ThreatDown K-12 Bundle promises:

- **Accelerated deployment across your diverse endpoint fleet**: We designed ThreatDown K-12 Bundle 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, Chromebooks, iPads, 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**: Advanced technologies include: EDR, next-gen AV, anti-exploit, device control, vulnerability assessment, patch management.
- **Contextualized 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.
- **24x7x365 fully managed services**: Included in the K-12 Bundle, Managed Detection & Response provides continual human-expert monitoring, threat hunting, and remediation services to empower your district to achieve cyber resilience. Our elite team of security analysts effectively closes your security resources gap and reduces your risk of unknown threats to increase your security efficiency exponentially.

Learn More

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.

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

Learn more

[i] Levin, Douglas A. (2022). "The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report." K12 Security Information Exchange (K12 SIX).
[ii] Threat intelligence team. (2023). "Ransomware Review: February 2023." Malwarebytes Labs.
[iii] Lyngaas, Sean. (2023). "Ransomware attack closes schools in Nantucket." CNN.
[iv] Source: Education Week, 2023.
[v] Multi-State Information Sharing & Analysis Center (MS-ISAC). (2022). "K-12 Report: A Cybersecurity Assessment of the 2021-2022 School Year." Center for Internet Security (CIS).
[vi] Sotnikov, Ilia. (2018.) "How to Perform IT Risk Assessment." Netwrix.
[vii] Federal Bureau of Investigation (FBI). "How We Can Help You: Ransomware." FBI.gov.
[viii] (2020.) Lessons in Cybersecurity. Malwarebytes.
[ix] Verizon 2022 Data Breach Investigations Report.
[x] Reinheimer, Benjamin et al. (2020.) "An Investigation of Phishing Awareness and Education over Time: When and How to Best Remind Users." USENIX.
[xi] See x.
[xii] See x.
[xiii] KnowBe4 Education Case Study.
[xiv] Bridgehead IT. "Best Practices for Endpoint Detection and Response."
[xv] ServiceNow. (2020.) "Costs and Consequences of Gaps in Vulnerability Response." Ponemon Institute.

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