PONDURANCE

What Schools Should Consider When Choosing an MDR Provider

The education industry, including K-12, community colleges, and universities, has experienced a difficult couple of years with COVID-19 restrictions, remote learning, curriculum debates, and funding concerns. Schools also can add cyberattacks and data breaches to that list.

Public school districts from Baltimore County, Maryland, to Broward County, Florida, to Fort Worth, Texas, have experienced ransomware attacks. Notably, in the Broward County attack, the cybercriminals demanded $40 million, though the district did not end up paying that extraordinary amount. Also, colleges and universities in states from California to Kansas to Massachusetts have been burdened with data breaches and ransom demands. Overall, the average cost of a data breach in the education industry totaled $3.79 million, according to the IBM Security *Cost of a Data Breach Report 2021*.[1]

OVERALL, THE AVERAGE COST OF A DATA BREACH IN THE EDUCATION INDUSTRY TOTALED

$3.79 MILLION

- IBM Security Cost of a Data Breach Report 2021

But there are security solutions that can help your school defend its data and protect against cyberattacks. Managed detection and response (MDR) is a growing category of security solutions, and technological research and consulting firm Gartner projects that 50% of all organizations will use MDR services by 2025.[2]

After reading this guide, you will have a better understanding of why schools are turning to MDR service providers for help. This guide covers:

- Cybersecurity challenges for schools
- Differences between SIEM, managed security service providers (MSSPs), and MDR
- How to evaluate an MDR provider
- The Pondurance approach to MDR

CYBERSECURITY CHALLENGES FOR SCHOOLS

The sheer number of potential threats is a large problem for schools trying to implement a security solution. Malware, ransomware, business email compromise, phishing schemes, and distributed denial-of-service attacks are all threats facing schools. Every school wants effective cybersecurity, but schools find it particularly challenging to deal with the expanded attack surface from remote learning and the costs and obstacles of building an in-house security operations center (SOC).

- **The expanded attack surface.** As schools have adapted to remote learning, students and teachers have found themselves using internet-connected devices such as laptops and tablets to communicate. Each device has expanded the attack surface, providing vulnerable points of entry for cybercriminals to penetrate the networks. With such vulnerability, proper cybersecurity protocols are required to keep out the bad actors or at least detect them if they are already within the network.

  Cyberattacks through the expanded attack surface threaten student safety and data privacy, cause learning disruptions such as school closings and disabled networks, and add overhead costs associated with IT and cybersecurity improvements. Learn five ways students and teachers can help to stay safe online.

PONDURANCE

- **Building (and retaining) an in-house SOC.** The costs and obstacles of building an in-house SOC affect schools at every level. Cybercriminals are increasingly smarter about circumventing prevention tools, making the cyber tools that your team used in the past no longer sufficient to detect phishing or ransomware attacks. You also need humans to defend against motivated bad actors. But technology tools are expensive to purchase and maintain, and cybersecurity professionals are in short supply and difficult to retain. As a result, many schools lack 24/7 detection and response capabilities.

Cybersecurity challenges your school may be experiencing:

- Shortage of cybersecurity talent
- Lack of visibility across the enterprise
- Security technology that is difficult to maintain
- Difficulty managing multiple tools and investigating all alerts
- Technology alone isn't enough to stop motivated attackers
- New compliance, privacy, and regulation requirements
- Undocumented processes in the event of an attack or breach
- Security professionals who are expensive to hire and hard to retain
- Inability to quickly remediate or reduce attacker dwell time

Overall,
51%
of organizations operate their SOC only during business hours.[3]

85%
of all breaches involved a human element in 2021, according to Gartner.[4]

PONDURANCE

DIFFERENCES BETWEEN SIEM, MSSP, AND MDR

Each type of security solution offers something unique and can fit different needs, but there's coverage overlap between some offerings that can make it difficult to know which solution to choose. Let's take a look at the three most popular security solutions on the market today:

- **SIEM.** Supports threat detection, compliance, and security incident management through collection and analysis of security events.
- **MSSP.** Provides outsourced monitoring and management of security devices and systems.
- **MDR.** Provides remotely delivered, modern, 24/7 SOC capabilities to rapidly detect, analyze, investigate, and actively respond to threats.

64%
of all organizations receive 5,000-plus alerts every day.[5]

Many schools may already have SIEMs in place for logging and alerting purposes. While the sheer volume of information gathered may be helpful, most schools can't deal with the overwhelming number of alerts that SIEMs generate. MSSPs offer some aid for information overload, but they often don't provide the comprehensive detection and response capabilities required to deal with modern threats.

MDR, on the other hand, offers the visibility provided by SIEMs and aids schools in managing security infrastructures and responding to threats.

MDR may be the answer for your school. Learn more about the differences between SIEM, MSSP, MDR, and Pondurance MDR in our comparison chart.

HOW TO EVALUATE AN MDR PROVIDER

When looking for a new MDR provider, you want to find the one that works best for your school. Gartner suggests that you consider an MDR provider if you need remotely delivered, modern, 24/7 SOC functions and there are no existing internal capabilities or if you need to accelerate or augment existing capabilities. Also, you should consider MDR if there is no one in-house to respond to threats that require immediate attention.

We recommend asking the following questions when evaluating an MDR provider:

- **Experience in education.** Does the provider have experience in the education industry? Does the provider work with other schools that are similar in size to yours?
- **Technology stack.** Can your MDR provider integrate with your current technology stack? Can the provider enhance your security operations while leveraging your existing IT investments?
- **A right fit with your policies.** Does the MDR provider's containment approach integrate with your school's policies and procedures? Does the provider fit with your current security protocols?
- **Monitoring of on-premises and cloud assets.** Does the MDR provider monitor across all your IT environments?
- **Custom reports.** Does the MDR provider offer custom reports including those needed for compliance and privacy?
- **Real-time alerts backed by human intelligence.** Does the MDR provider have a fully managed and monitored log? Does the provider offer real-time alerts?
- **Incident response and remediation.** Does the MDR provider offer incident response capabilities? Will the provider work with you to respond to threats across your network, log, endpoint, and cloud environments? Can the provider help minimize losses and prevent future incidents?

PONDURANCE

THE PONDURANCE APPROACH TO MDR

Pondurance detects, responds to, and remediates cyber threats for schools, regardless of size or current in-house capabilities. We stand apart from other MDR services in how well we integrate with existing security systems, deliver expert-driven monitoring and response, and use advanced tools to aid in analysis and forensics operations. We combine our advanced technology platform with human intelligence to protect and defend schools against cyberattacks.

- **MDR.** Pondurance provides 24/7, U.S.-based SOC services powered by analysts, threat hunters, and incident responders who use our advanced cloud-native platform to provide continuous cyber risk reduction. By integrating 360-degree visibility across network, log, endpoint, and cloud data and with proactive threat hunting, we reduce the time it takes to respond to emerging cyber threats.

  Pondurance MDR is the proactive security solution backed by authentic human intelligence. Technology is not enough to stop cyber threats. Human attackers must be confronted by human defenders.

- **Incident response.** When every minute counts, schools need specialized cybersecurity experts to help them respond to a compromise, minimize losses, and prevent future incidents. Pondurance delivers digital forensics and incident response services with an experienced team capable of guiding you and your school every step of the way. This includes scoping and containing the incident, determining exposure through forensic analysis, and helping to quickly restore your normal operations.

A REAL-WORLD SUCCESS STORY

The Joplin School District in southwestern Missouri saw other school districts falling victim to ransomware attacks. The district was using legacy cybersecurity tools to keep more than 7,000 students and their internet-connected devices safe from a cyberattack. However, it didn't feel the tools were proactive enough to protect the network. The district was looking for a 24/7 security solution with an automated and assisted response from an in-cloud SOC. Find out how Pondurance MDR successfully solved the cybersecurity issues for the Joplin School District.

Want to learn more about MDR and what it can do for you?

Dive deep into the subject in the first-ever Managed Detection and Response for Dummies eBook. Read more.

Sources:
1. Cost of a Data Breach Report 2021, IBM Security, 2021.
2. Market Guide for Managed Detection and Response Services, Gartner, Oct 2021.
3. Unraveling Threat Detection and Response Solutions, 451 Research, 2021.
4. 2021 Data Breach Investigations Report, Verizon, 2021.
5. 2020 Cisco Benchmark Report, Cisco, 2020.