PONDURANCE

What Schools Should Consider When Choosing an MDR Provider

pondurance.com

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. But there are security solutions that can help your school defend its data and protect against cyberattacks.

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**

Overall, the average cost of a data breach in the education industry totaled

$3.79M

according to the IBM Security *Cost of a Data Breach Report 2021.*[1]

PONDURANCE

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

Shortage of cybersecurity talent

Lack of visibility across the enterprise

Security technology that is expensive and hard 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 that are expensive to hire and hard to retain

Inability to quickly remediate or reduce attacker dwell time

PONDURANCE

What's the best option for schools: SIEM, MSSP, or 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.

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.

64% OF ALL ORGANIZATIONS RECEIVE **5,000-PLUS** ALERTS EVERY DAY.[2]

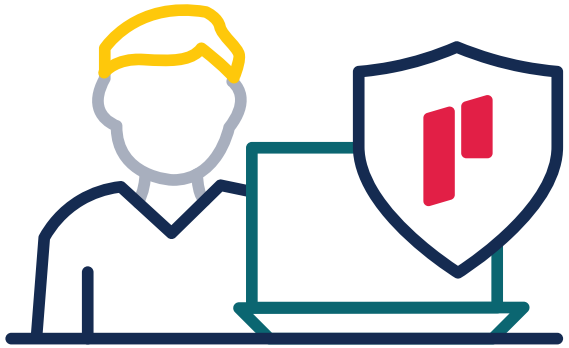
MDR may be the answer for your school. **Learn more about the differences between SIEM, MSSP, MDR, and Pondurance MDR in our comparison chart.**

How to evaluate an MDR provider

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?

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.

PONDURANCE

PONDURANCE

500 N. MERIDIAN ST., STE. 500
INDIANAPOLIS, IN 46204

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to clients seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.

Sources:

1. Cost of a Data Breach Report 2021, IBM Security, 2021.
2. 2020 Cisco Benchmark Report, Cisco, 2020.

pondurance.com