School District Improves Its Cybersecurity Posture With Managed Detection & Response

PONDURANCE

CASE STUDY

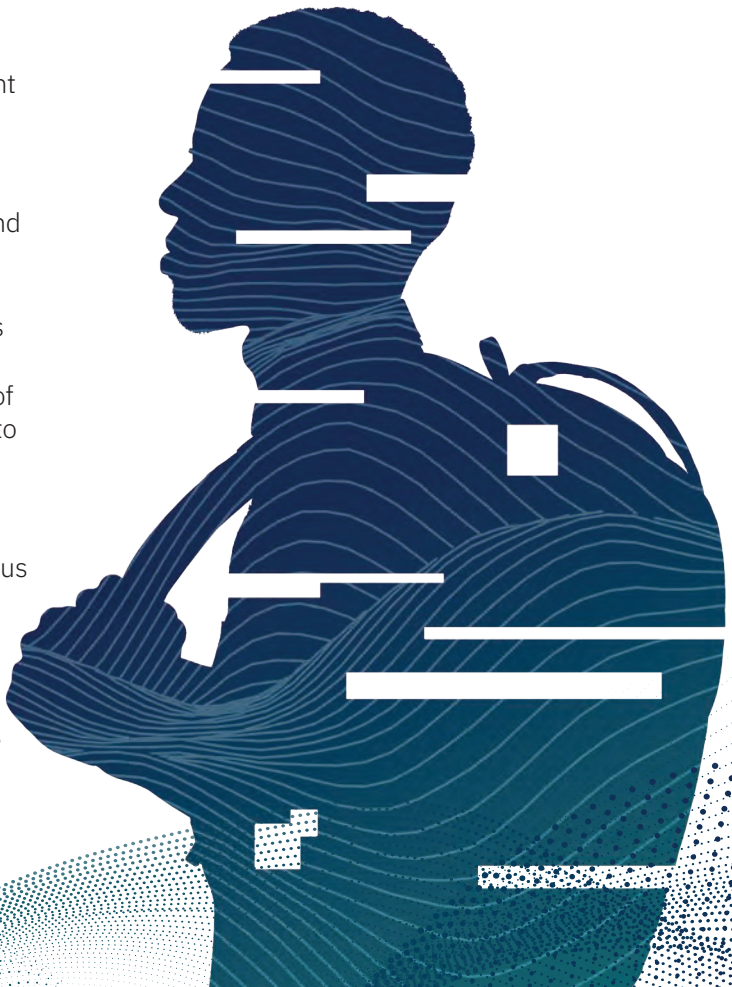
THE CHALLENGE

Members of a school district serving grades K-12 came to us knowing that they had work to do to improve their cybersecurity posture. They were using legacy cybersecurity tools like a next-generation firewall with an intrusion prevention module, antivirus on endpoints, and basic vulnerability patching. They saw multiple municipalities and school districts falling victim to ransomware attacks. The network administrator for the school district wanted to be proactive and make sure that they school district was not the next victim on the news due to a lack of visibility and response capability. The network administrator and their team are responsible for keeping technology operational and secure so that the school district can educate over 7,000 students.

> **We know we have a huge attack surface and there are many ways a cybercriminal could gain access to our network. My assumption is that we can never prevent malware from getting into our network. We need the tools in place to detect malware as it's attempting to spread through our network and be able to take an active response. We are not manned 24/7; we were looking for a product that would have an automated and assisted response from an in-cloud SOC provider that could take action off-hours and on weekends.**
>
> —School District Network Administrator

OUR SOLUTION

Pondurance Managed Detection and Response (MDR) was the right fit for the school district. Our MDR platform is able to ingest endpoint, log, network, and Internet of Things (IoT) data through a combination of an Endpoint Detection and Response (EDR) platform, network sensors, and a log collector. We monitor data and respond to threats detected from their tech stack consisting of enterprise-grade HP/Aruba, VMware, and Microsoft products, as well as a range of other internet-connected devices like Smart TVs and Chromebooks. All the data that is ingested across the environment is analyzed and correlated against multiple sources of threat intelligence, enabling our security operations center (SOC) to detect, investigate, and respond to any threats or unusual activity. The school district has a robust network of over 7,000 student devices, 1,000 staff devices, and 20 servers that are needed to deliver education across the district. Handling response to malicious findings across that many endpoints is a significant challenge so it made sense for the school district to include SentinelOne, an EDR platform. SentinelOne gives Pondurance's SOC deeper visibility to investigate indicators of compromise, including signatures, recorded or alerted by the endpoint to gain a better analysis of the potential threat.



pondurance.com

500 N. Meridian St., Suite 500, Indianapolis, IN 46204

Copyright © 2024 Pondurance

School District Improves Its Cybersecurity Posture With Managed Detection and Response

PONDURANCE

CASE STUDY

THE RESULTS

The school district now has 24/7 monitoring with immediate reaction from Pondurance's SOC. The district evaluated other leading cybersecurity products and services to compare capability, comprehensiveness, and alignment to its needs. Pondurance MDR was the best overall solution with the most comprehensive coverage at an optimal total cost of ownership. The school district's IT leadership ultimately saved the district money and resources by adopting Pondurance MDR rather than trying to procure, integrate, manage, and monitor its own individual technologies. Hiring staff to provide 24/7 coverage to detect and respond to cyber threats can cost several multiples of the cost of Pondurance MDR. Overall, the school district spent less than $200,000 annually to fully protect its network and bring the students and staff peace of mind.

> "We wanted an MDR that could protect more than our Windows and Mac operating devices. We have a lot of IoT devices and Chrome devices like Chromebooks. Pondurance's network solution gives good coverage for IoT through a network sensor and network log aggregation. This gives a total network view of threats that are developing and might be trying to spread."
>
> —Assistant Network Administrator

BENEFITS OF PONDURANCE MDR SERVICES

- Stop security incidents through 24/7 detection and response
- Allow the SOC team to take immediate action to isolate infected devices and protect the network
- Maximize internal resources and security investments
- Improve compliance through reporting
- Increase visibility into alerts that require action
- Rapidly accelerate security program maturity
- Lower total cost of ownership

ABOUT PONDURANCE

Pondurance delivers world-class MDR services to industries facing pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation.

Our advanced platform with our experienced team of analysts continuously hunts, investigates, validates, and contains threats so your team can focus on what matters most.

pondurance.com

500 N. Meridian St., Suite 500, Indianapolis, IN 46204

Copyright © 2024 Pondurance