CASE STUDY

Logically
CYBER FIRST. FUTURE READY.

SentryXDR Helps the Education Sector Maintain Compliance with Frequently Changing Regulations

Technology is becoming ubiquitous in the education industry, resulting in rapidly expanding attack surfaces and increased targeting by threat actors.

With the average cost of a data breach in the education sector reaching nearly $3.7 million in 2023, colleges and universities are becoming laser-focused on data and network security to protect student and staff information and comply with frequently changing privacy laws and regulations.

Recently, Logically worked with a higher education institution that needed to quickly bring its cybersecurity protocols into compliance with newly updated Gramm-Leach-Bliley Act (GLBA) requirements.

Logically provided the organization with the 24/7 security monitoring, threat detection, and reporting capabilities it needed to comply with nine new GLBA elements and, in the process, significantly elevated the education provider's overall security posture.

Background

The Gramm-Leach-Bliley Act is a federal law that defines how financial institutions are allowed to collect, protect, access, and disclose an individual's private information. The GLBA also requires these institutions to explain their information-sharing practices to customers.

What does this have to do with the education sector? The GLBA defines financial institutions as "companies that offer consumers financial products or services like loans, financial or investment advice, or insurance." Because higher education institutions provide financial services and products—such as Perkins loans and other financial aid—they are required to comply with GLBA requirements.

When the new GLBA elements were released, the technology leadership at this educational institution knew they needed to enlist the help of cybersecurity specialists to bring their systems into compliance.

THE PROBLEM:

Tightening Security on a Tight Deadline

As the security landscape in the education sector continues to evolve, emerging threats are driving the need for new tools and technology to secure data and networks. In response to these new threats, GLBA released updated requirements to help ensure the security and confidentiality of student and staff information.

This educational institution complied with the existing GLBA requirements at the time. However, after the updated elements were released in late 2021, its cybersecurity strategy was found to be lacking a few critical components, including 24/7 monitoring of its network systems.

With only 18 months to upgrade its cybersecurity to meet the June 2023 deadline, the organization began looking for a security operations center (SOC) platform that could solve its immediate need for enhanced monitoring, detection, and analytics and be flexible enough to adapt to future regulatory changes.

THE SOLUTION:

SentryXDR Provides Unmatched Threat Detection, Actionable Intelligence, and Customer Experience

Before partnering with Logically, the client was evaluating the services of a security operations (SecOps) platform provider to bridge the gaps in its cybersecurity plan.

After comparing Logically's SentryXDR SOC-as-a-service (SOCaaS) solution with the other candidate's offerings, the client chose Logically due to its decades-long partnership with cybersecurity solutions provider SonicWall and ability to deliver next-level visibility, threat detection, and actionable intelligence across the client's network.

Here's how they measure up:

Service and Support

The other solution: Support tickets are submitted to a "concierge," then farmed out to many different technicians. There is no continuity of service.

SentryXDR: Logically's "white-glove" services and support include a fully trained technical team dedicated to supporting SentryXDR customers, so you can be confident that you are always working with specialists committed to delivering exceptional service.

Correlation and Analysis

The other solution: This solution uses connectors between devices to collect data and then send it back to a central engine for correlation and analysis.

This means analytics are solely based on data collected from devices/endpoints with connectors. If you want more data, you have to pay for more connectors.

SentryXDR: Powered by AI and machine learning, SentryXDR collects and correlates data streams from all relevant sources in your environment—network assets, Microsoft 365, endpoint detection and response—so you have a 360-degree view of your security operations center in a single pane of glass.

Market-Leading Technical Capabilities

Unlike other extended detection and response (XDR) platforms in the same space, SentryXDR offers a broad range of features that allow organizations to respond to threats quickly and efficiently, including:

- Fully integrated network and endpoint detection and response.
- File integrity monitoring for compliance, security, and remediation.
- Network segmentation and segregation monitoring and alerting.
- Adaptive models powered by machine learning to automatically tune out noise.
- Detection analysis with context and situational awareness.
- Real-time, continuous threat and breach detection powered by machine learning.
- Automated real-time threat remediation or push-button remediation with rollback.

THE RESULTS:

SentryXDR Bridges Security Monitoring Gaps and Future-Proofs Compliance

SentryXDR provides the client with the features and functionality it needs to stay in compliance with GLBA requirements today and in the future. Unlike the "other solution," SentryXDR will scale with the client as needs and requirements change.

In addition to filling in critical missing capabilities, such as 24/7 network security monitoring, Logically has delivered other essential services to help the client meet the GLBA requirements and increase its overall security posture, including:

- Security risk assessment
- Security awareness training
- Penetration testing

What's Next for Cybersecurity and Education?

The education sector is going all in on technology, introducing more vulnerabilities and opportunities for threat actors to circumvent traditional cybersecurity safeguards and exfiltrate sensitive personal data.

We can expect more rapid-fire changes to privacy protection laws to combat the rise in cybersecurity threats against educational institutions. Logically can help your organization pivot quickly to new regulations and implement the latest and most effective SOC solutions so you stay in compliance and your students' data stays secure.

Want to learn more about how SentryXDR is helping educational institutions leverage AI and advanced machine learning to build a comprehensive security posture?

Speak with one of Logically's cybersecurity experts today.

Speak with an Expert

Logically™
CYBER FIRST. FUTURE READY.