CASE STUDY

Health and Social Services Organization Uses Arctic Wolf to Keep Patient Records Safe

BUSINESS

The organization provides health and social services to children and adults with intellectual disabilities through community- and campus-based programs.

CHALLENGES

- Ensure robust HIPAA compliance
- Execute comprehensive security strategy in a complex IT environment with limited staff
- Demonstrate that PII and ePHI are protected

RESULTS

- SOC capabilities and expertise for less than the cost of one fulltime employee
- 1000's of alerts reduced to a few actionable incidents per week
- Customized reports to meet HIPAA compliance requirements

"The AWN CyberSOC™ service is far superior to anything offered by traditional MSSPs, and the level of service I get from my Concierge Security™ team is truly amazing. We selected Arctic Wolf because it provides a comprehensive package that included everything we needed at an affordable price. To build the equivalent of the service in-house would have cost 10X ."

Healthcare IT Director

One of the nation's oldest health and social services organizations has served children and adults with intellectual and developmental disabilities for more than 100 years. Throughout its history, the organization has pioneered new service models and developed new programs to meet the changing needs of people with disabilities and help them reach their full potential. This non-profit organization has partnered with local governments and communities to provide services across multiple states.

In the course of its business, the organization stores and transfers a good deal of confidential data related to patients and others. That's why it deployed Arctic Wolf's SOC-as-a-service to protect electronic patient health information (ePHI) and sensitive personal identifiable information (PII) across multiple service facilities.

Lack of Cybersecurity Expertise Creates Need for a SOC-as-a-Service

Like many midsized organizations, the healthcare services provider has a modest IT staff tasked with managing a complex IT environment. This means its engineers must assume several roles and have little time for hunting down security alerts generated by point security products deployed in the organization's IT infrastructure. Cybersecurity was not their forte, but the need to secure patient and client data became increasingly important with the rise of newer threats such as WannaCry ransomware.

Recognizing the gap in their expertise, the team weighed adding a managed security service provider (MSSP) solution, such as FireEye, against managing it in-house with Splunk Enterprise Security for security information and event management (SIEM). Their analysis showed they could not feasibly get all the services they needed from a traditional MSSP or an in-house SIEM without significantly increasing their budget and staffing.

Arctic Wolf's AWN CyberSOC™ service met their needs by providing a dedicated Concierge Security™ team (CST) that works as an extension of their IT team. The Arctic Wolf CST is their singular point of contact, monitoring their network and directing response to all threats. With years of security experience to draw from, the organization relies heavily on the CST's expertise in handling its security-related matters and ensuring its data stays safe.

Addressing Alert Fatigue

The IT team had a good perimeter defense architecture in place, including next-generation firewalls, web gateways, and a mobile device management solution. The challenge was that each of these point solutions generated thousands of alerts per day. The IT staff had no time to investigate and determine which were legitimate security incidents. With so many alerts, alert fatigue can set in, where IT staff become so desensitized to the noise they fail to respond to an actual threat.

The AWN CyberSOC service ingests thousands of daily alerts from the organization's wide range of security products and highlights only those few that require some sort of remediation. The service combines machine intelligence to correlate incoming alerts with network flow data, behavioral analytics and threat feed subscriptions, and a dedicated CST to perform validation and triage. Additionally, the AWN CyberSOC includes unlimited log collection, so daily triage and forensics are performed across the entire network.

Dedicated Security Expertise and 24/7 Monitoring

The organization's IT team was impressed by the AWN CyberSOC service and Arctic Wolf's DNA, especially for the following reasons:

- A dedicated AWN Concierge Security team that acts as an extension of the organization's IT staff, and is always available as a trusted security advisor
- A predictable, fixed monthly service cost for continuous network monitoring with expertise for threat detection and response, which was far more cost-effective than deploying a SIEM
- Arctic Wolf is an engineering-driven company that continually invests in its cloud-based SOC-as-a-service platform to meet customer demands

Arctic Wolf: A Trusted Cybersecurity Partner

This health and social services organization found Arctic Wolf to be a trusted SOC-as-a-service provider, with a dedicated security team that understands its specific business risks (protecting PII/ePHI data) and provides customized reports to meet its compliance requirements. As a midsized non-profit organization with a small IT team, Arctic Wolf brought it peace of mind through expert 24/7 monitoring that's become essential for growing non-profit organizations.

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com