ARCTIC WOLF

BETHESDA

PERSONAL | PREDICTABLE | PROTECTION

CASE STUDY

Bethesda Health Group Gains Security Visibility and Strengthens HIPAA Compliance with the Arctic Wolf SOC-as-a-Service

At a Glance

Bethesda Health Group
bethesdahealth.org
provides exceptional senior living care and services through its retirement communities, skilled nursing home communities, and home and community-based programs in the St. Louis area.

Challenges

- Limited security expertise to support geographically-dispersed locations
- Lack of comprehensive cybersecurity visibility
- Compliance with HIPAA HITECH healthcare mandates

Results

- Comprehensive visibility across all locations and resources
- Flexibility to adapt to a changing environment
- Reporting to help achieve compliance

> "Arctic Wolf's turnkey SOC-as-a-service provides us with advanced threat detection and response capabilities at a fraction of what it would cost to do it ourselves. The Arctic Wolf Concierge Security™ model works perfectly for our IT team, which previously had no dedicated security resources."
>
> **— Joshua Sharp,** Director of Information Technology, Bethesda Health Group

Protecting Residents' Personal and Health Information

Bethesda Health Group is the premier provider of senior care and services in St. Louis. It operates 14 independent living, assisted living, and skilled nursing and memory facilities in the St. Louis area. While it seeks to maintain an optimal security posture to minimize risk to sensitive data of both the organization and its residents, Bethesda is also required to comply with the Health Insurance Portability and Accountability Act (HIPAA) and must ensure that appropriate processes are in place to maintain compliance.

With more than 1000 employees, Bethesda's IT infrastructure includes more than 700 workstations and laptops, 100+ servers, 100+ routers and switches, and 1500+ Active Directory (AD) accounts for users located in all 14 physical locations. Overseeing the network and the organization's many SaaS applications provided quite a security challenge for the company's small IT team since it didn't have a dedicated security engineer on staff. Instead, that responsibility was spread among several staff members who had no formal security training, nor did they have the necessary tools in place to allow them to efficiently monitor the environment and take timely action on the security alerts. This proved to be a very inefficient and labor intensive process. The volume of alerts in an organization Bethesda's size can be overwhelming, so identifying all the incidents that required immediate action was a daunting task for this team. Management knew they needed to identify a solution quickly.

Protecting sensitive patient data required for HIPAA compliance was also a key challenge for Bethesda. The organization needed reporting to demonstrate compliance with HIPAA HITECH mandates for electronic protected healthcare information. With all this in mind, Bethesda considered different options for monitoring and responding to security events. Rather than building their own security operations center (SOC) on premises, however, the IT team selected the Arctic Wolf SOC-as-a-service.

Deployment was simple, straightforward, and completed in minutes. The Arctic Wolf sensor arrived preconfigured and was ready to plug into the network to collect logs and network flow data. And Bethesda's IT team worked with Arctic Wolf's Concierge Security™ Team to customize the service to fit its exact operational and security requirements.

Outstanding Results Across the Board

Bethesda saw some immediate benefits from the service. The IT team quickly discovered:

- Users were visiting a known malicious site
- Endpoints sending out traffic that appeared abnormal
- A phishing attack that compromised corporate Dropbox credentials

Prior to the Arctic Wolf SOC-as-a-service's deployment, the team couldn't investigate these potential indicators of compromise. Each of these threats was detected and researched by the Concierge Security Team, which presented Bethesda's IT team with a clear action plan on how to reduce or eliminate the risk. Today, the Arctic Wolf SOC-as-a-service provides the highest level of security, identifying potential threats while avoiding the noise of false positive alerts.

Just as important, Arctic Wolf helped Bethesda reach its HIPAA compliance goals by adapting to Bethesda's changing environment. The burden of generating reports for senior management and compliance was alleviated using Arctic Wolf SOC-as-a-service 's standard and custom reporting. Weekly external assessments on the public-facing infrastructure provides Bethesda with vulnerabilities that need to be addressed. And regularly scheduled security posture reports provide senior management the peace of mind that the organization always has vigilant cybersecurity.

Arctic Wolf has delivered Bethesda advanced security at far less cost than if it had built a security operations center in-house. Around-the-clock SOC staffing would require eight to 12 security engineers alone. In fact, the cost of the service is estimated to be a small fraction of the cost of deploying and managing a SOC internally.

ARCTIC WOLF

SOC2 Type II Certified

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com