CASE STUDY

Arctic Wolf Cures Madison Memorial Hospital's Security and Compliance Pain

BUSINESS

Madison Memorial Hospital (www.madisonmemorial.org) provides professional compassionate care for five counties in eastern Idaho. Madison is a community-owned, nonprofit hospital that focuses on the needs of the community with an excellent maternity center, surgical centers, and more.

CHALLENGES

- Constrained IT resources and limited cybersecurity expertise
- Monitoring a diverse environment, including endpoints, servers, and medical devices
- Compliance with the Health Insurance Portability and Accountability Act (HIPAA)

RESULTS

- Comprehensive visibility across all resources supported by the IT team
- Flexibility to adapt to a changing environment and ingest new data sources
- Robust reporting that helps ensure HIPAA compliance

"Arctic Wolf removes a big security burden for our organization. Locating, training, and retaining security personnel would be a major challenge for us, so Arctic Wolf's Concierge Security™ team is invaluable in helping us improve our security posture and meet compliance obligations."

Rhett Jackson, Executive Director of Facilities and Information Systems, Madison Memorial Hospital

Safeguarding Patient Health Information and Hospital Infrastructure

Madison Memorial Hospital is a 69-bed hospital with 580 employees located in Rexburg, Idaho. Its facilities include a main campus, an offsite clinic, and two adjacent office buildings. The Madison IT team consists of 20 members across multiple teams, including one specialist focused on information security and compliance. The team must manage and monitor a diverse infrastructure that includes about 600 endpoints, nearly 300 servers, network infrastructure with a variety of switches, routers and wireless access points, and several thousand medical devices.

Although Madison had a fairly robust security infrastructure, an external risk assessment had highlighted Madison's need to improve its cybersecurity practices, particularly with regard to incident detection and response. The hospital also has compliance requirements driven by the Health Insurance Portability and Accountability Act (HIPAA). According to Rhett Jackson, executive director for facilities and information technology, "In some of our HIPAA audits and assessments, we received red flags around the need to monitor logs from servers, workstations, and devices. We knew we had to find a solution that would raise our security posture and help meet HIPAA compliance requirements."

A Two-Fold Goal: Improve Cybersecurity While Fulfilling Compliance Obligations

The hospital did not have a solution to holistically monitor its infrastructure and detect threats when it began considering available options. It quickly realized what it needed was a security operations center (SOC). Before long, the team narrowed the decision between three SOC approaches to meet the security need: (1) using an on-premises security information and event management (SIEM) solution, (2) leveraging a managed security service provider (MSSP), or (3) deploying a managed detection and response (MDR) service. After evaluating SIEM products from Splunk and Exabeam, and an MSSP offering from SecureWorks, Madison decided on Arctic Wolf's SOC-as-a-service—the AWN CyberSOC™ service.

"The more we looked at on-premises SIEM technologies—which included a pilot SIEM deployment onsite—the more we realized the amount of resources that would be needed to manage it," said Jackson. "We were very impressed by the other solutions. However, tuning a SIEM, sifting through false positives, and updating rules would be a challenge given our current staffing resources. An on-site deployment would require the hiring of several full-time employees as we couldn't risk having such expensive technology become shelfware."

The numbers told the story. "We calculated the total cost of ownership over a five-year period for outsourcing the SOC using Arctic Wolf versus bringing it in-house with another technology," Jackson added. "The cost of doing it in-house was almost double." Money, however, wasn't the only issue. "With some of the other options we considered, it seemed like they were designed for organizations that had far more internal resources. Arctic Wolf takes most of the security burden off of our hands. We get customized security from a team that understands our environment."

Constantly Improving IT Health

Madison was able to quickly deploy the AWN CyberSOC™ service and gradually increased the amount of data directed to it. And the hospital has continued to improve its cybersecurity posture by remediating issues raised by Arctic Wolf's Concierge Security™ team.

"The dashboards and reports we receive are really good summaries that provide a clear picture of what happens in our environment," said Jackson. "It's reassuring to see things that we normally wouldn't know about. We get a report on outstanding vulnerabilities, we get them remediated, and the next report reflects our efforts along with any new vulnerabilities. We know that our security posture is constantly improving."

The AWN CyberSOC's monitoring provides Madison with better visibility of its environment. While many alerts are ultimately discovered to be false positives—such as too many password tries from mistyping—Jackson said, "It is reassuring that we now know whether it's from legitimate user error or someone outside trying to compromise credentials. In the past, we simply would not know about it but now have visibility into these types of activities. It gives us confidence that when we do get attacked, Arctic Wolf will alert us."

Cost savings is also a significant factor since turning to Arctic Wolf. Both in terms of staff and resources. "We are a relatively small organization as far as in-house security personnel, and we really rely on Arctic Wolf," said Jackson. "The Concierge Security team has been extremely timely and very professional with a high level of expertise. They communicate clearly with us, so that we can act quickly. This helps tighten down our environment."

Madison encountered the occasional virus outbreak prior to deploying the AWN CyberSOC service, and the cost to recover from these outbreaks had increased as malware dwelled for longer periods in the hospital's environment. "We were really concerned with our ability to respond when attacks happen," Jackson said. "In the past, it took many hours, if not days, to deal with the effects of viruses. Users can't work if their files are corrupted, data is lost, or their system is inaccessible. While we have good backups, restore processes, and disaster recovery in place, we prefer to avoid large-scale recovery. Arctic Wolf can quickly identify and remediate attacks to reduce the impact when something hits."

Arctic Wolf also provides Madison with the flexibility to evolve its IT operations and take advantage of Arctic Wolf's security monitoring for software-as-a-service (SaaS) applications, which is something the hospital is now considering. As Jackson explained, "Arctic Wolf has helped us avoid the need to purchase three or four different outside services. We now have the simplicity of a single service that combines a SIEM, intrusion detection, vulnerability scanning, and incident response. Arctic Wolf keeps it simple for us and allows us to improve our security posture at a reasonable cost. The value we get far exceeds anything we had previously considered."

ARCTIC WOLF

AICPA SOC

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com