BURKE REHAB HOSPITAL

Customer profile

Provider of in-patient and out-patient rehabilitation medicine in New York State.

Industry

Healthcare

IT environment

Burke Rehab Hospital has one primary physical location and 10 satellite sites in the region. The organization's 1,100 employees use managed corporate devices, including networked medical equipment, servers, and peripherals.

BURKE REHABILITATION HOSPITAL EXPLORES VAST POTENTIAL OF ARMIS SOLUTIONS

Armis shines a light on network-connected devices across IT and clinical settings and monitors data traffic to better secure patient information

Burke Rehab Hospital is a leading provider of in-patient and out-patient rehabilitative care in New York State. The security team knew they needed to up their game in the area of network security. After deploying Armis, they were able to expand their visibility into devices connecting to the network, monitor device utilization across the organization, and view unencrypted and encrypted traffic to detect and prevent patient data exfiltration. Burke Rehab continues to discover new use cases for Armis that enhance security and provide operational insights across the entire organization.

CONNECT WITH US

BURKE REHAB HOSPITAL CASE STUDY ©2022 ARMIS, INC.

Burke Rehabilitation Hospital in White Plains, New York, is a member of the Montefiore Health System network and is a top-tier leader in rehabilitation medicine. In operation for over a century, the healthcare provider offers in-patient services to patients at its 150-bed adult acute care facility and out-patient services through an extensive network of healthcare facilities across the region. Burke offers rehabilitation care for neurological, musculoskeletal, cardiac, and pulmonary conditions resulting from illness, injury, or surgery.

Security team looks to Armis to upgrade network security

Director of Network Operations and Security Brian Schultz, who has been with Burke Rehab for 10 years, is always on the lookout for innovative and robust solutions to enhance the organization's security. He's a hands-on, nuts-and-bolts leader, heading up a team of 14 IT and security professionals. On the heels of completing a SANS Institute training class on looking at data traffic and intrusion prevention, he learned about Armis from a reseller, who informed him about the many capabilities of the solution. That conversation set the wheels in motion for a Proof-of-Value (PoV) and later deployment.

"One of the reasons we decided to give Armis a try is because we found we were lagging in the area of network visibility. Our existing network control (NAC) solution wasn't able to provide granular details about devices plugged into our environment or how they were interacting with each other. Other solutions we had looked at would have taken a substantial level of effort to implement. Armis appeared to be a good alternative for us because it immediately provided us with visibility into what devices were plugging into the network. It shows us how they are interacting with each other, creates alerts based on observed behavior and enforces firewall rules based on those alerts," says Schultz.

Why packet inspection is critical

Schultz tested Armis against a competitor and discovered that the competing product was only providing network data in the form of log files rather than inspecting network traffic packets. The Armis appliance, on the other hand, sits out of band and uses Switch Port Analyzer (SPAN) ports to passively monitor traffic without impacting network performance. It does deep-packet inspection, providing information about the type of traffic flowing through the network, including anomalies and identification of both encrypted and unencrypted traffic. This is especially important in the healthcare sector, which is subject to strict regulations with respect to the privacy of patient data from Health Insurance Portability and Accountability Act (HIPAA) and other agencies. For example, Armis can detect a device that is sending unencrypted medical images. It then sends an alert to security teams so they can take further action to address the risk.

"If you can see packets, that's the ultimate. There's no sense in looking at log files," observes Schultz. "We are looking at Armis as a new way to gain insights into our network. It only takes a little bit of effort on our part to get an enormous amount of information. Prior to Armis, the amount of work it would take to collect that data would be beyond our capabilities."

Challenges

- No visibility into devices on the network
- Device sprawl, with many computing clinical devices exhibiting low usage
- Inability to detect suspicious or risky traffic, resulting in weak data and network security

"We are looking at Armis as a new way to gain insights into our network. It only takes a little bit of effort on our part to get an enormous amount of information. Prior to Armis, the amount of work it would take to collect that data would be beyond our capabilities."

Brian Schultz
Director of Network Operations and Security
Burke Rehab Hospital

Armis zeroes in on low-utilization IT and medical devices

Another one of Schultz's key IT initiatives is containing server sprawl. He and his team are leveraging Armis to see the network traffic on the servers across the organization in order to determine the level of utilization. With this information in hand, they can retire servers that are no longer needed. Prior to Armis, he points out, it would take an immense amount of time to run scans on server usage with one of their legacy products.

As a consummate technician deeply involved with the backend of operations, Shultz knows that Armis can provide useful, cost-saving information on device utilization. For example, the Armis team built a query so that Schultz and his team could see which vital carts were being used by clinical staff. Vital carts are portable digital, network-connected devices that enable medical staff to collect patient data such as blood pressure and respiration rates. These carts typically come with displays, scanners, and printers.

"Armis allowed us to see whether some of the vital carts that seemed to be collecting dust in the corner were actually being used," he explains.

Burke Rehab has a shared services model with the Montefiore Hospital network and connects with the parent organization's network to use its electronic medical record (EMR) system. In this context, Armis provides added value by identifying how effectively the devices they are sharing are utilized and what the costs are.

Stronger security through vulnerability detection and integration with investigation tools

Armis has also detected high-profile Apache Log4j vulnerabilities in Java logging frameworks. This flaw enables attackers to execute code remotely on a targeted device, which means they can steal data, install malware, or take control of the device. Apache Log4j hacks are particularly prevalent in medical devices. This vulnerability has even compelled the FDA to raise this issue with medical manufacturers.

Schultz is also involved in basic security incident investigations and uses CrowdStrike for that purpose. While CrowdStrike is installed on all devices that use agents, there are blind spots on devices that cannot use agents. Integration of CrowdStrike with Armis has opened up additional visibility and enabled deeper investigations across a wider cross-section of devices.

Armis opens up opportunities for new use cases

While Schultz and his team are still in the early stages of exploring Armis, they are well aware that the potential use cases for Armis are nearly boundless. They are currently focused on illuminating what's on the network and on identifying legacy equipment that's no longer being used to full capacity and are excited about other creative applications for the solution. For example, Schultz has plans in the near future to employ Armis to manage network performance by checking deviations in network protocols, which can be leading indicators of data exfiltration.

Armis Results

- Broader visibility into both rogue and new Internet of Things (IoT) and medical devices that connect to the network
- Insights on usage to determine which devices—from servers to peripherals to medical equipment—are truly adding value to the organization and which ones can be retired
- Integration with CrowdStrike to enable deeper investigations when suspicious events arise
- Detection of both encrypted and unencrypted network traffic for better protection of patient data and other regulated healthcare information
- Big payoff in proportion to the amount of effort required to deploy and manage Armis

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

info@armis.com

20221404-1

BURKE REHAB HOSPITAL CASE STUDY ©2022 ARMIS, INC.