CASE STUDY

Armis Discovers More Than Double the Number of Known IT and IoT Assets at Memphis Utility Company

The Challenge

- Lack of a complete view into IT and IoT assets
- No reliable way to identify network-connected unmanaged and rogue assets
- Inability to pinpoint and remediate vulnerabilities
- Disparate security solutions that slowed detection and remediation of threats and vulnerabilities

The Solution

- Implemented Armis Centrix™ for Asset Management and Security for IT and other departments
- Integrated Armis with 11 solutions in the security stack
- Received in-depth training to get the most out of the Armis platform

The Results

- Provided a comprehensive and accurate asset inventory of all IT and IoT assets
- Discovered more than twice the number of assets previously accounted for
- Drilled into the security posture of assets, speeding up vulnerability mitigation
- Reduced time and effort involved in troubleshooting and issue resolution

Industry: Utilities

Location: Memphis, Tennessee

Number of Employees: 3,500 in 100+ locations near Memphis

Armis Centrix™ for Asset Management and Security

Background

Founded in 1852 during the Civil War era, Memphis Light, Gas and Water (MLGW) is now the largest three-service municipal utility in the country. MLGW is headquartered in Memphis, Tennessee and provides reliable and affordable electricity, natural gas and water service to more than 440,000 customers across Shelby County. The utility company purchases electricity from the Tennessee Valley Authority and natural gas from various transmission companies. Unlike other utility companies that draw water from lakes or rivers, MLGW taps into the Shelby County aquifer, a deep underground natural source known for its purity containing more than 100 trillion gallons of water.

The corporate network infrastructure at MLGW encompasses a broad array of IT and IoT assets: PCs, servers, virtual machines, switches, routers, and firewalls, along with scanners, cameras, TVs, and back-up uninterruptable power. To better secure and manage assets in this complex environment, Supervisor, Information Technology, Missy Burkes needed a tool that provided true visibility into unmanaged and rogue devices while accelerating cybersecurity mitigation by identifying vulnerabilities.

"We had no trouble convincing our executive team that Armis was the ultimate solution we had been looking for."

"During the PoC, when Armis found so many unmanaged and rogue IT and IoT assets on our network that we had not been aware of—everyone was sold on its effectiveness as both an asset and vulnerability management tool."

Missy Burkes,
Supervisor, Information Technology, Memphis Light, Gas and Water (MLGW)

The Solution

Burkes learned about Armis Centrix™ for Asset Management and Security at a local workshop. Impressed with the scope of asset and vulnerability information that Armis provides, she prepared a presentation on its capabilities to upper management and won buy-in immediately.

"We had no trouble convincing our executive team that Armis was the ultimate solution we had been looking for," said Burkes. "During the PoC, Armis found so many unmanaged and rogue IT and IoT assets on our network that we had not known about. Everyone was sold on its effectiveness as both an asset and vulnerability management tool."

Unlike competing solutions that monitor assets that use standard network protocols, such as SNMP, Armis finds any asset that has an IP address. This provides more accurate and complete information on unmanaged and IoT assets that don't support these protocols.

"Armis fulfilled this requirement, providing us with accurate information on asset location, connectivity to specific network switches that we may not have been aware of, and vulnerability status for assets that needed updates or should be retired," explained Burkes.

The Results

For Burkes, the primary use cases for Armis are twofold: getting comprehensive visibility and detailed insights into connected IT and IoT assets and resolving critical incidents. Armis serves as a single source of truth, offering real-time insights into both permitted and unsanctioned assets. Before Armis, the asset count was 5,600. Armis identified more than 13,000.

"Armis lets us know when users are putting things on the network without permission. It not only helps us mitigate vulnerabilities, but also disable assets or stop them from communicating on the network," said Burkes.

Integrations with 11 technologies in the security stack—including Splunk, Tenable, Device42, Lansweeper, and Trend Micro endpoint protection—further enhance visibility by surfacing insights in a single pane of glass. This unified view enables Burke's team to prioritize risks and proactively mitigate threats and vulnerabilities faster. When incidents arise, her team no longer has to swivel between multiple security consoles to gather the data they need to resolve issues.

The Armis Centrix™ platform's easy-to-use query tool and its intuitive visual dashboard have also greatly accelerated issue detection and remediation. "When we're in a troubleshooting situation, we can easily identify a problem and provide a detailed report to upper management in just minutes. In these scenarios, we've substantially reduced the amount of time we spend on these tasks. Before Armis, it would take us 30 to 45 minutes to zero in on a problem. Now it takes us two minutes or less," said Burkes.

Burkes has extended Armis to other departments at MLGW, giving them the ability to monitor their equipment in real time. This enables teams to detect anomalies, potential threats, and vulnerabilities, such as outdated firmware.

"Armis points out to them that, 'Hey, this is something serious, and your equipment should be under review.' They can act quickly to research and fix issues, making the environment more resilient against cyberthreats," remarked Burkes. The Armis platform's dashboard clearly displays information such as security posture gaps and hidden risks.

Armis University Training has also proven invaluable for Burke and her staff and has helped them deepen their technical knowledge of the platform's capabilities. These hands-on sessions provide practical labs with real-world scenarios and best practices, complete with playback recordings for later review.

Looking ahead, Burkes plans to explore how Armis can help track and better secure the utilities' OT environment. Due to stringent compliance specifications, OT assets are isolated in a separate network to protect the critical infrastructure from potential threats.

"We're still in the early stages, but, as we dive deeper into the Armis platform, we look forward to expanding its footprint at MLGW," noted Burkes. "I wholeheartedly recommend the platform to any organization that wants to improve its security posture and the efficiency of its team."

132%

more IT and IoT assets discovered on the network

50%

reduction in time to asset discovery

11

integrations, including Splunk, Tenable, VMware, Trend Micro, and more

Troubleshooting reduced from **45 minutes to 2 minutes**

ARMIS.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011
www.armis.com