CASE STUDY

City of Jonesboro Secures Critical Infrastructure and Boosts Cyber Resilience with Armis Centrix™

The Challenge

- Difficulty gaining visibility into IT and OT environments
- Struggling to manage a growing number of connected devices
- Limited resources to address cybersecurity risks
- Need to protect critical public infrastructure from cyberattacks

The Solution

- Deployed Armis Centrix™ across IT and OT networks
- Integrated Armis Centrix™ with existing security tools
- Implemented real-time monitoring and threat detection
- Provided enriched data to the city's CMDB for better asset management

The Results

- Discovered and secured 30% more assets
- Reduced time spent on manual device identification
- Enhanced threat detection across both IT and OT networks
- Improved the city's cybersecurity posture with proactive monitoring

Industry Government

Location Jonesboro, Arkansas

Size 500+ employees

Armis Centrix™ for Asset Management and Security

"Armis gave us the complete visibility we needed across both IT and OT environments. We discovered 30% more devices than we thought we had, which has transformed how we secure our city's critical infrastructure."

Jason Ratliff
Director of Information Systems, City of Jonesboro, Arkansas

Background

The City of Jonesboro, located in northeast Arkansas, is home to over 80,000 residents and serves as a regional hub for industry, healthcare, and education. The city government spans 23 different departments with approximately 700 employees, along with a 911 center that supports both the city and Craighead County.

The city's IT department, led by Director of Information Systems Jason Ratliff, is responsible for maintaining the network infrastructure and cybersecurity across multiple municipal facilities, including water treatment plants, government offices, and public safety services.

In recent years, Jonesboro has faced increasing cybersecurity challenges as the number of connected devices in its IT and OT environments has grown. From municipal IoT devices, such as security cameras and traffic lights, to critical OT assets, such as water treatment control systems, the city's attack surface has expanded rapidly. Managing these assets and securing them from cyberthreats has become a priority.

The Challenge

The City of Jonesboro struggled to maintain full visibility over its expanding network of devices. Jason Ratliff and his team were tasked with ensuring that all connected assets were properly monitored and protected, but with hundreds of unmanaged devices, this was no small feat. The lack of comprehensive asset discovery tools left gaps in the city's security, particularly in its operational technology (OT) environment, where the critical infrastructure controlling water treatment and other public services was at risk.

"We had a huge blind spot when it came to our OT devices," Ratliff explained. "We didn't clearly understand what was connected to our network, which made it difficult to protect those assets."

30%

more devices discovered and secured across IT and OT networks

Hours of manual asset identification reduced to seconds with automated visibility

Real-time monitoring across critical infrastructure with 24/7 threat detection

100%

improvement in visibility of OT assets, including public utilities

In addition to visibility challenges, the city's IT department was limited in terms of resources. Manually tracking devices, identifying vulnerabilities, and ensuring security controls were up to date was both time-consuming and prone to error. Jonesboro needed a risk management solution that could automate these processes while providing real-time insights into their security posture.

The Solution

After seeing Armis Centrix™ in action at a conference, Ratliff was impressed with the granular visibility and intelligence it provides. The City of Jonesboro deployed Armis Centrix™ for Asset Management and Security to address these challenges. Armis was able to provide deep visibility across both IT and OT environments, discovering and securing assets that had previously gone unnoticed.

"With Armis, we were able to identify 30% more devices on our network than we initially thought we had," said Ratliff. "This gave us a clear and comprehensive view of both our IT and OT environments, allowing us to better secure our city's critical infrastructure. Being able to see all the assets on the network with all the details, including firmware versions, model numbers, and patching status was a game changer for us."

Armis Centrix™ integrated seamlessly with the city's existing security tools and infrastructure, including their configuration management database (CMDB). By enriching the CMDB with detailed, real-time data on device status, vulnerabilities, and network behavior, the IT team was able to quickly prioritize and address security risks and hone threat-hunting efforts.

The platform's flexible and non-intrusive nature, including agentless deployment options, was particularly beneficial for the city's OT environment, allowing the IT team to monitor critical infrastructure without disrupting sensitive systems. Armis provided continuous, passive monitoring of devices and detected anomalies in real time, helping the team respond proactively to potential threats.

The Results

Since deploying Armis Centrix™, the City of Jonesboro has significantly improved its asset visibility and security posture. The platform enabled the discovery of 30% more devices than were previously known, including critical OT assets, which have since been either upgraded or patched with the latest security updates.

The automation provided by Armis Centrix™ has reduced the amount of time spent on manually identifying and tracking devices, freeing up valuable resources for the IT team. "We used to spend hours just trying to figure out what was on our network. Now, with Armis, we have that information in seconds," Ratliff said.

In addition, Armis helped the city enhance its threat detection capabilities. The platform continuously monitors both IT and OT networks for suspicious activity, flagging potential risks before they escalate into full-blown incidents. This has been critical in protecting the city's infrastructure from cyberthreats, particularly as the number of cyberattacks on public utilities continues to rise.

"Armis has given us peace of mind," Ratliff noted. "It's like having a flashlight in a dark room. We can now see everything, secure everything, and manage our cybersecurity risks effectively. It's an invaluable tool for a city like ours, and I would highly recommend it to any city government IT organization."

ARMIS®

1.888.452.4011
www.armis.com

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..