ARMIS

WALTON COUNTY SCHOOL DISTRICT

Case Study

K-12 School District Deploys Armis Across 15 Schools to Protect IoT and OT Assets Against Malware Attacks

The Challenge

- Gaining full visibility into IoT and OT assets
- Identifying unauthorized and unknown devices in the environment
- Bolstering security posture to prevent malware attacks
- Adhering to the Center for Internet Security (CIS) framework version 8.1
- Working within the financial budget available for the district

The Solution

- Deployed Armis Centrix™ for Asset Management and Security and Armis Centrix™ for Early Warning
- Installed 15 collectors, one at each school, across the district
- Integrated the Armis platform with 42 other tools

The Results

- Gained immediate visibility into the district's environment and asset estate
- Identified 30,000+ assets—twice as many as expected
- Discovered suspicious and unauthorized connections and rogue devices
- Enhanced the patch management process by zeroing in on potential vulnerabilities
- Eliminated major pain points by adhering to the CIS framework
- Saved time and reduced workload
- Enhanced overall security posture

Industry: K-12 Education

Location: Atlanta, Georgia

Size: 2,500

Armis Centrix™ for Asset Management and Security

Armis Centrix™ for Early Warning

Background

Walton County School District serves approximately 14,500 students across 15 schools and operates a highly diverse technology environment. In addition to managed devices such as laptops, phones, and Google Chromebooks for students, the district has multiple unmanaged IoT and OT assets, including BYOD, security cameras, access control systems, thermostats, HVAC controllers, and occasional rogue devices.

Cyber Security Analyst Kyle Kobos is responsible for the district's cybersecurity stance. He and his network engineer are tasked with responding to security incidents and taking proactive measures, with a focus on blocking ransomware threats.

"I was very excited to get Armis in the environment. It's so quick and easy. The day we received the collectors, I put them in the back of my truck and went out to each and every school that same day and put them in place."

Kyle Kobos,
Cyber Security Analyst,
Walton County Schools

The Challenge

An expanding attack surface proliferating with IoT and OT assets was the driving factor in the decision to onboard the Armis platform. "We take a defense-in-depth approach to knowing where critical data is," Kobos explained. "It became clear we needed to extend that same approach to knowing where our critical assets are too."

Because staff often bring personal devices into schools to support and enhance student learning, Kobos identified potential security vulnerabilities associated with this practice. For instance, an instructor might bring an Alexa device and connect to the network using staff credentials.

Frequently, outside vendors also bring in devices that pose security risks. "We knew there was a dark side to our network that we didn't quite understand, and it scared us, because the unknown devices could potentially lead to a successful malware attack," Kobos pointed out. At the time, he didn't have a clear idea of how many assets and what assets were on the network, particularly IoT and OT devices.

"With the increase of attacks against K-12 districts, it's really important that we harden our defenses to prevent ransomware and other advanced malware attacks," Kobos remarked. One of the district's goals is to achieve strict adherence to the Center for Internet Security (CIS) Critical Security Control, version 8.1 framework, which introduces a new "Govern" function. Identifying where assets were located and used was especially challenging during the CIS control implementation.

Another challenge was budget constraints and leadership buy-in—a common issue in the education sector.

The Solution

The district deployed Armis Centrix™ for Asset Management and Security and Armis Centrix™ for Early Warning across all 15 schools, installing one collector at each school.

The deployment was easy, straightforward, and quick. Originally scoped as a three-month project, it took Kobos only three weeks to get Armis deployed, configured, and integrated.

"I was very excited to get Armis in the environment," Kobos recalled. "The day we received the collectors, I put them in the back of my truck and went out to each and every school that same day to install them," he said.

As part of the rollout, Kobos integrated Armis Centrix™ with 42 other tools, including network mapping solutions, patch management tools, Microsoft Active Directory, Dynamic Host Configuration Protocol (DHCP), a Remote Monitoring and Management (RMM) tool from PDQ Connect, a security integrations tool from Pinnacle Systems, and a Google Chrome OS integration. Additional integrations are planned as the program matures.

Kobos explained that he uses integrations to enrich the Armis data as much as possible and provides a comprehensive view into both north-south and east-west traffic. They make it possible to get visibility into unmanaged devices that are only being viewed by Switched Port Analyzer (SPAN) and Network Test Access Point (TAP).

"Security is not convenient. It's not easy, but it's necessary in today's world. If there is any way we can simplify it and make it easier for the team, we should—and Armis is helping us do just that."

Kyle Kobos,
Cyber Security Analyst,
Walton County Schools

The Results

Armis Centrix™ delivered immediate visibility into the district's full asset estate, revealing a much larger environment than expected. Before Armis Centrix™, the district believed it had about 2,500 managed computers and 14,000 Chromebooks. Armis Centrix™ identified more than 30,000 total assets, nearly double the expected number. "It was a real wake-up call for us," said Kobos.

Armis Centrix™ also identifies suspicious connections from personal devices and rogue devices, enabling Kobos and his team to take rapid action on these unauthorized assets. For example, they detected a camera that appeared on the network and discovered that it was from a manufacturer they did not recognize. With Armis Centrix™, they located the campus where the camera was installed and immediately took it offline.

Armis Centrix™ also strengthened patch management. The team takes pride in their patch management system, but, due to agent issues and data gaps, a large number of unauthorized Adobe Flash Player instances had gone undetected. "Armis Centrix™ allows us to identify all the potential vulnerabilities," said Kobos.

Moreover, Armis Centrix™ allows Kobos and his team to treat unmanaged devices as though they are managed. Armis Centrix™ for Early Warning leverages the cloud-based Armis Collective Asset Intelligence Engine to analyze crowd-sourced data gathered from all over the world and prioritizes vulnerabilities based on this threat intelligence.

"Not only does Armis Centrix™ tell you what's going on in your environment and what assets are there, Armis Centrix™ for Early Warning alerts you to the vulnerabilities that are tied to those devices and shows the traffic activity," he observed. "We're not just getting a spreadsheet—we're seeing what vulnerabilities need to be prioritized because they're actively being used by attackers in the wild right now."

The platform also proved valuable during lifecycle transitions. When Windows 10 was deprecated and replaced by Windows 11, the IT team needed to replace all its insecure Windows 10 assets. Armis revealed 30 to 50 Windows 10 devices that were still connected to the network through Simple Network Management Protocol (SNMP) connection. Without Armis Centrix™, it would have taken days and even weeks to discover these assets. Many were owned by third-party vendors and public agencies that had not appeared in internal inventories. This allowed the district to proactively coordinate updates and reduce exposure.

Armis Centrix™ played a critical role in advancing Walton County's alignment with the CIS framework. "Armis Centrix™ was central to Controls 1 and 2," Kobos noted. Asset visibility and governance had been a struggle, but Armis Centrix™ filled that gap and made the job easier by identifying both hardware and software assets and providing granular reporting capabilities.

Looking ahead, Kobos plans to build a sustainable vulnerability management program using Armis Centrix™ for Early Warning and Armis Centrix™ for VIPR Pro - Prioritization and Remediation. Currently he and his network engineer are handling the remediation work, but his future plan is to share the workload with his team. With Armis Centrix™, he can quickly delegate remediation tasks by cross-referencing Armis Centrix™ for Early Warning data with how those vulnerabilities would affect the largest subset of machines in the district. "It's a win-win. Not only are we staying secure, but we're reducing the workload and we're being more efficient," Kobos remarked.

15
collectors installed across the district

42
integrations connected in the Armis platform

3 weeks
to complete deployment

30,000+
devices identified on the network

For Kobos, the return on investment is clear. “The biggest return for us is security,” he stated. “It’s hard to put a price on that,” he remarked. He noted that Armis Centrix™ enables proactive risk mitigation rather than reactive, costly recovery—and this, ultimately translates to cost savings.

Through Armis’s partnership with Georgia Leaders of Educational Technology (GLET), a non-profit technology resource organization for the state of Georgia, the district was authorized to acquire Armis Centrix™. “That was the golden ticket for us that finally put an elite security tool within our budget,” shared Kobos.

Kobos has the goal to make the district more secure every day. “Security is not convenient. It’s not easy, but it’s necessary in today’s world. If there is any way we can simplify it and make it easier for the team, we should—and Armis is helping us do just that.”

ARMIS

See how leading organizations secure their environments with Armis.

See Armis Centrix™ in Action

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

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 safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011
armis.com