CASE STUDY

United Airlines Uses Armis Centrix™ to Decrease OT Cybersecurity Risk

With a categorized OT asset inventory, United Airlines stays a step ahead of potential threats and regulatory directives

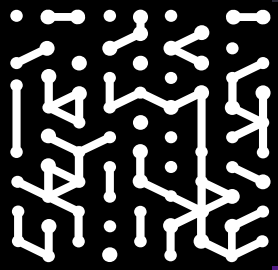
United Airlines

Industry

Aviation transportation

IT Environment

Approximately 100,000 employees and a large global OT asset estate



United Airlines operates in a highly regulated industry with new directives around cybersecurity expected to be forthcoming. Armis provides the organization with an up-to-date operational technology (OT) asset inventory of every device on the network. This helps the airline stay ahead of the curve in terms of compliance and can decrease risk to the organization overall

Headquartered in Chicago, Illinois, United Airlines is the third largest airline in the world by fleet size and number of routes. With over 800 planes, it operates regular flights to all six inhabited continents, serving 342 destinations in 48 countries.

The airline's cybersecurity and digital technology teams are located in the Chicago area and Houston, Texas. Chris Peters, the principal architect for operational technology and industrial control system cybersecurity, has worked with the company for a little over a year and a half and has over 15 years of experience in cybersecurity. He is focused on maintaining security for the organization's sprawling network of OT devices — in seven hubs spanning Chicago, Los Angeles, San Francisco, Houston, Chicago, and other locations.

Describing the scope of his responsibilities, Peters said, “Not everyone realizes this, but United Airlines owns a lot of the equipment at the airports. If you walk out to the O’Hare International Airport terminal where we have a hub, and you walk into Terminal 1, you’ll see a jet bridge that we own.” United Airlines also owns many of the physical systems at the airports, such as air conditioning, bag conveyors, bag scanners, motors, controllers, and the like—all part of a sprawling OT network.

According to Peters, the OT security team did not have a clear idea of all the devices in the OT network. The traditional network monitoring tools that were in place were not designed to build a comprehensive inventory of OT hardware and software. He acknowledged that, while it was possible to manually ping the IP addresses of every single known device and start analyzing its function and what it was communicating with, that would have been a monumental task.

Following a successful proof-of-value (PoV), United Airlines deployed Armis Centrix™. Peters and his team found that the agentless Armis platform offers a more accurate, faster, and easier way to locate OT assets, such as process control devices, switches, cameras, and more. It collects information such as device type, manufacturer, model, location, and more, along with valuable metadata such as connections, traffic, alerts, and vulnerabilities. This rich asset data makes managing OT inventory easier for Peters and his team.

Integrations add even more value

Peters notes that the most useful part of Armis Centrix™ when it comes to OT is its ability to do raw network analysis. “But that’s not everything that [Armis] does,” he added. “It also uses integrations and can collect data from our existing tools. The network mapper that uses the SNMP protocol can crawl around

Challenges

- Building a complete and accurate OT asset inventory
- Categorizing OT assets
- General need to decrease risk to the organization

and quickly tell you that there's something connected to a switch."

Peters and his team have also integrated Armis Centrix™ with endpoint detection tools, vulnerability management tools, policy engines, and virtual hosts.

Visibility is crucial in a post-Colonial Pipeline world

The desire to increase visibility into the airline's vast asset estate amid continuing escalating cybersecurity concerns of a cyberattack also drove deployment of Armis Centrix™. Peters pointed out that the Colonial Pipeline ransomware attack was a turning point for professionals in his field. "The whole operational technology cybersecurity genre is new ever since Colonial Pipeline. We're all growing together," he remarked.

On May 7, 2021, Colonial Pipeline, which owns the largest pipeline system for refined oil products in the U.S., was hit with a ransomware attack that took out the billing infrastructure of the company, forcing it to shut down operations as a precautionary measure to prevent further attacks. The shutdown led to fuel shortages, panic buying, and a state of emergency being declared across the Southeastern United States.

Just five days after the attack, President Biden issued a 15-page executive order entrusting multiple federal agencies with the task of strengthening cybersecurity through several new initiatives. Part of the directive was for the National Institute of Standards and Technology (NIST) to provide guidelines and best practices, which are aimed largely at federal agencies, though other industries are now using the NIST framework for risk assessments, including many airlines.

Armis Centrix™ Results

Armis Centrix™ is helping United Airlines to improve its OT security posture and protect its critical infrastructure from cyberattacks.

- Provided deeper visibility into the large OT asset estate
- Enhanced security posture
- Helped prepare for new regulation and compliance requirements
- Prioritized vulnerabilities for the incident response team

“If you pull up any risk assessment framework, NIST 853 or whatever framework you want to use, the very first line is always focused on visibility,” said Peters. He added, “I just heard [a global food producer] had a ransomware incident that took out their production. So if you don’t want that to happen to your organization, the first step is to identify where those key assets are, what they’re doing, and what they’re communicating with,” he said. With Armis, Peters is now even better equipped to initiate investigation and remediation in the event of such an attack.

Increasing regulation in OT cybersecurity

Peters is seeing a growing trend in his industry towards more regulation. On October 18, 2022, the Transportation Security Administration (TSA) announced a new cybersecurity directive that regulates railroad carriers. Peters expects that a similar directive will come along for airlines, so he is looking carefully at the regulations.

The TSA railroad directive requires that railroad carriers take action to prevent disruption and degradation to their infrastructure, describing specific ways in which they must improve security. Two directives relate to vulnerability management and asset visibility—and that is where Armis Centrix™ fits into the picture. One requirement is continuous monitoring and detection capabilities to detect threats and anomalies that could affect critical system operations. Another requirement is keeping operating systems, applications, drivers, and firmware up-to-date with security patches, using a risk-based methodology.

Peters plans on using Armis Centrix™ to prepare for future directives for the airline industry. “You need to be taking inventories at certain dates. You need to be logging traffic. And you need to have baselines for the network to be able to understand if there’s a deviation. That’s where Armis will come into play,” he said.

Armis Centrix™ helps separate the signal from the noise

Apart from the directives, it was a “general desire to improve the organization’s risk profile” that led Peters to deploy Armis Centrix™, with future compliance needs in the back of his mind. “We asked to see visibility of every device in the network, and we got what we asked for,” he said. “One day, I remember our asset inventory went from about 100,000 devices to over 3 million devices. We’ve since pared that back,” he added. “Part of the value of [Armis] is understanding what’s important. For example, do we really need to know that a Nintendo switch came within Wi-Fi distance of one access point in one airport? Probably not.”

Describing his initial experience of seeing Armis in action, Peters said, "You don't expect to have that much information ready that quickly." He explains that it's a process to fine-tune the alerts and figure out what needs to be prioritized.

"You might see a vulnerability and then find out it's completely isolated and maybe not even accessible. Do we really consider that as critical, or should we focus on other things? I think it's extremely useful to get to the first third or maybe half of where you want to be. Once you know all these vulnerabilities exist, you need to figure out what to do about them. And that requires you to pivot quickly and build a larger program based on the risks that [Armis] shows you."

Armis Centrix™ proves to be more than just an asset inventory tool

Though the airlines is primarily using Armis Centrix™ to identify and catalog its OT assets, Peters has found other applications for Armis. He points to a regulation that applies to camera placements at airport locations. Peters said, "You could dispatch a service person to check out the airport once a month, or you could ping every device once a month. But it certainly would be easier if you had an intelligence tool to do that for you. Armis has vastly simplified and expedited this process."

The ability to do rich queries in Armis Centrix™ valuable for Peters in unexpected ways. He noted, "I can ask Armis to show me a device that has a certain MAC address that connects to a certain subnet launched from a particular virtual host that was connected to by a user with a specific role. So it's not just OT. It can be useful in many other places." Peters discovered that Armis Centrix™ can find non-ethernet-connected things, such as devices connected to building management systems, which typically use the BACnet communication protocol.

"It's phenomenal to be able to say to a network engineer who needs to know where all of the industrial switches are, 'I can tell you that in about two seconds.'"

"The most useful part of Armis Centrix when it comes to OT is its ability to do raw network analysis. But that's not everything that Armis Centrix does, it also uses integrations and can collect data from our existing tools. The network mapper that uses the SNMP protocol can crawl around and quickly tell you that there's something connected to a switch."

Christopher Peters
Principal Architect, United Airlines

With Armis Centrix™ for IT/IoT security organizations can secure cyber-physical assets by achieving full visibility across converged IT, OT, IoT .

See, secure and manage critical assets and critical infrastructure using the industry's most advanced cyber exposure platform.

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

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial