CASE STUDY

Major U.S. Cultural Institution Protects Its Valuable Historical Archives With Armis

Gains full visibility into its IoT network and an integrated, end-to-end security infrastructure.

United States Cultural Institution

Industry

Not-for-profit historical institution funded by the U.S. government and private donors.

IT Environment

Amazon Web Services (AWS) public cloud, VMware private cloud, and network IoT devices.

With two million visitors to its physical location and 25 million visitors to its website each year, the U.S. Cultural Institution in Washington, D.C. serves an important role in preserving and sharing critical and sensitive historical artifacts.

Introduced and managed by security firm Trofi Security, Armis has evolved into the single dashboard for the firm’s many security tools, providing full visibility into the institution’s vast Internet of Things (IoT) estate and automating routine security analyst tasks.

Trofi Security is an information security firm located in Lafayette, Colorado and headed by Michael Trofi. The firm operates as the virtual CISO and provides security operations center (SOC) services for the U.S. Cultural Institution in Washington, D.C. Since its dedication on April 22, 1993, the institution has had 47 million visitors and is home to more than 50 million artifacts, archival documents, photographs, archival footage, library items, and oral history testimonies. Part of the collection includes 1.25 petabytes of single source archives, meaning that the institution holds the only copy in the world. With such a valuable asset estate to protect, “risk management is very important,” explained Trofi.

Trofi Security was initially contracted by the institution eight years ago to perform a risk assessment, which later led to the U.S. Cultural Institution becoming the firm's largest client. Other clients include local governments, technology companies, and financial institutions. The firm offers virtual CISO and CTO services, security operations center (SOC) services, risk management, penetration testing, and regulatory compliance.

Armis provides critical visibility into the large IoT network

The firm had many tools in place for managing vulnerabilities and for monitoring east-west traffic on the network but needed a way "to tie those two together," explained Trofi. "Armis was brought in to help us identify where all our IoT devices were, in conjunction with Checkpoint, our firewall vendor," he explained. "Visibility is very important. You can't fix it if you don't see it, and we had no idea where the devices were. Armis helped us solve that problem," he added.

The institution's IoT assets include sensors to monitor light, humidity, and temperature around its vast collection of art and artifacts, as well as cameras, printers, televisions, door alarms, entry sensors, and HVAC devices. After a quick proof-of-value (PoV) that identified "a lot of gaps" and showed "instantaneous" value, as Trofi puts it, Armis discovered over 100 IoT devices on the network, which the team at Trofi Security was not previously aware of.

Armis serves as a single dashboard for all the other security tools

In addition to the initial use case for asset discovery, the Armis deployment quickly expanded into more use cases.

Challenges

- Seeing what devices are on the network
- Staying on top of patches and updates
- Boosting overall security posture

Trofi Security integrated Armis into the firewalls, vulnerability scanners, and endpoint detection and response (EDR) tools. “It became a one-stop shop,” asserted Trofi. “I think Armis is the only tool we have that’s actually pulling [data] from all the other security tools through integrations,” he explained. “It has become our single dashboard.”

A big benefit the team is deriving from the Armis deployment is time savings. “We’re integrating the Armis Enterprise Workflow Automation (EWA) module with Torq.io security automation software and other security orchestration, automation, and response (SOAR) software. Armis goes to Slack channels for notification, it opens a ticket in our ServiceNow digital workflow management software, and then it actually sets the rules in our EDR software and blocks something. That’s perfect,” exclaimed Trofi.

Armis eliminates lower-tier security tasks, taking the burden off the Trofi team

Like many organizations in the security space, Trofi shared that staffing fast enough and with the right people is a major challenge—as is getting the budget to do so. Consequently, he is always looking for ways to automate the “lower-tier of the pyramid,” referring to routine security analyst tasks. “All these retainable tasks are playbooks that Armis helps initiate and that we can now automate. I can assign those resources to do something else that’s more important. That’s the value-add with all these integrations.

All the security vendors should be going down this road with open APIs [application programming interfaces],” he observed.

Trofi estimates that, because of the automation workflow and time-saving capabilities of Armis, he’s been able to eliminate a full-time security analyst position. “Instead of somebody sitting there all day, looking through logs, it’s all automated,” he said.

Armis Results

- Makes it easy to see which devices need patches
- Blocks problematic devices from accessing the network
- Prevents future security incidents
- Saves substantial time and effort

Secondary use cases further extend the value of Armis

Network performance and connectivity is another use case where Armis is making a difference. “Armis helped us find out that our VPNs were misconfigured. Instead of going to the closest domain controller, they were actually going to the one farthest away. We had a lot of retransmissions,” explained Trofi. The team is also using Armis to block queries to known malicious sites, TikTok, and BitTorrent connections. In particular, Trofi is concerned about large bulk uploads from devices that shouldn’t be uploading data. The U.S. Cultural Institution has seen many cyberattacks from both rogue and state-sponsored actors, and the threats it faces are intensifying and evolving in sophistication.

“Armis will help us detect a threat from unusual east-west traffic,” explained Trofi.
It’s also helping Trofi Security get a tighter rein on their application access control lists (ACLs), which document permissions associated with system resources. “Things grow organically, and nobody ever goes back to clean things up. We’re starting to see a lot of that in the dashboards,” shared Trofi. Recently, Armis discovered that the U.S. Cultural Institution’s store upgraded all its card swipers without informing the security team. “Armis caught it because all the IPs changed,” said Trofi. Next, he intends to use Armis to monitor payment card industry (PCI) compliance.
In terms of customer service and support, Trofi said he received the “white-glove” treatment from the Armis staff. “Armis technical support has been better than most companies we deal with. They always go out of their way to help us,” he said. “And deployment was really simple. Armis is one of the easiest products I’ve ever worked with.”

“I think Armis is the only tool we have that’s actually pulling [data] from all the other security tools through integrations. It has become our single dashboard.”

Michael Trofi
CISO, Trofi Security

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