Case Study

# Armis Enables Full Asset Visibility and Policy Enforcement at Grand Canyon University

## The Challenge

- Creating an accurate, up-to-date, and comprehensive asset inventory across a large sprawling campus, along with many satellite locations
- Identifying critical assets and connectivity in a systematic way
- Discovering and prioritizing vulnerabilities
- Streamlining and enhancing the purple team test process

## The Solution

- Deployed Armis Centrix™ Asset Management and Security with collectors in key data centers
- Integrated Armis with all security and infrastructure tools
- Passively discovered vulnerabilities for prioritization and remediation
- Enabled purple team incident response testing from a single pane of glass using simple search queries

## The Results

- Provided complete and continuous visibility and asset management across the entire environment
- Discovered 100+ assets that lacked endpoint detection and response (EDR) security agents
- Enforced security agent compliance across all assets
- Updated remediation roadmap to align with risk priorities
- Saved time when conducting purple team exercises
- Improved overall cybersecurity hygiene

**Industry:** Higher education

**Location:** Phoenix, AZ

**Size:** 6,500 faculty and staff

**Armis Centrix™ for Asset Management and Security**

## Background

Grand Canyon University (GCU) is a private Christian university in Phoenix, Arizona. Established in 1949 as Grand Canyon College, the university offers degrees in more than 200 areas of study across nine colleges, including multiple technology-focused certifications and degrees. Focusing on preparing students to work in cybersecurity fields, GCU prioritizes its Cyber Center of Excellence, a classroom on campus where students can learn about and practice different techniques. Additionally, its immersive Overclock cybersecurity residence program gives students the opportunity to practice ethical hacking and defense skills in a simulated “live” corporate environment. As of September 2023, GCU enrolled more than 100,000 students online and in person—a significant expansion from its 2008 enrollment of fewer than 1,000 students—making it one of the world’s largest Christian universities.

The university’s infrastructure has grown alongside its burgeoning student body, ushering in a host of technical and security challenges. After one of GCU’s vendors was involved in a supply chain attack, CISO Michael Manrod researched that category of assets in the university’s technology stack. He discovered these devices were in a corporate network zone, instead of being walled off in an isolated segment, in line with policy. Although the university’s environment was not compromised, this triggered an initiative to get its asset management house in order.

"Armis is essential to our cybersecurity strategy. Before Armis, we made policies, we checked, we scanned, and we hoped. With Armis, we know."

**Michael Manrod,**
**CISO, Grand Canyon University**

Manrod and his team of 25 technology professionals led the university's effort to better assess and safeguard a complex IT and IoT environment that includes security cameras and badge readers as well as more traditional assets such as servers and user endpoints.

## The Challenge

Grand Canyon University lacked unambiguous, comprehensive insight into its assets—what assets were connected to the environment, where they were located, which ones were communicating with what and how, and what kinds of risks were associated with each type of asset. This created multiple blind spots in its approach to vulnerability management, leading to uncertainty about the extent to which its environment was protected.

The university's IT team also had no simple, centralized way to enforce rules and policies, such as those pertaining to which IoT devices should be cordoned off in designated server zones.

This exposed the university to zero-day threats and other attacks that could disrupt essential services. It also hampered the IT team's ability to effectively uncover and prioritize risks.

GCU knew it was time to find a solution that was easy for everyone, including IT interns, to learn and use.

## The Solution

GCU installed Armis sensors at all its data centers and integrated the Armis solution with its 25 security and infrastructure management tools, giving the IT team a single, consolidated, real-time view of asset and user data through Armis Centrix™ for Asset Management and Security. With complete, end-to-end visibility into the university's communication flows and the ability to map assets to critical business systems and services, the university is now empowered with a clear and actionable "record of truth."

Once GCU decided to go with Armis, the rest was easy. The Armis solution integrated with the university's existing technology stack through out-of-the-box API connectors; no custom integrations were required.

In fact, Manrod said his team's experience with getting Armis up and running was among the easiest installations they have ever been through. "The deployment was truly seamless," said Manrod. "The Armis UI is easy to understand, and the APIs and integrations were clean and well-defined—they just worked. We rely on Armis to find problems in our environment instead of waiting for adversaries to do so."

## The Results

Armis enables GCU's IT team to gain a holistic view into its entire ecosystem, root out rogue assets, apply protocols uniformly and comprehensively, and prioritize its remediation roadmap according to the risks associated with each type of asset. The team is empowered to improve GCU's overall security hygiene and more easily and efficiently manage and secure its large asset inventory.

"Armis enables us to see what we couldn't confirm with our existing toolset. "It figures out what assets we have, where they are, and what they are communicating with. Armis helps us build a to-do list of what to fix in our environment. This means we can now better prioritize and focus on resolving vulnerabilities and other issues efficiently. It enables us to keep everything

**100+**
**unprotected assets identified**

**100%**
**asset visibility**

**25**
**integrations completed**

patched and secure. Without Armis, we almost certainly would have missed those problems," said Manrod.

As a case in point, he pointed out that Armis immediately identified more than 100 assets in the university ecosystem that lacked proper EDR security agents.

The Armis platform also serves as a verification and enforcement tool, ensuring that the team can quickly validate that GCU's security policies are fully enforced. It shines a light on issues and anomalies, enabling the IT team to address them quickly and efficiently.

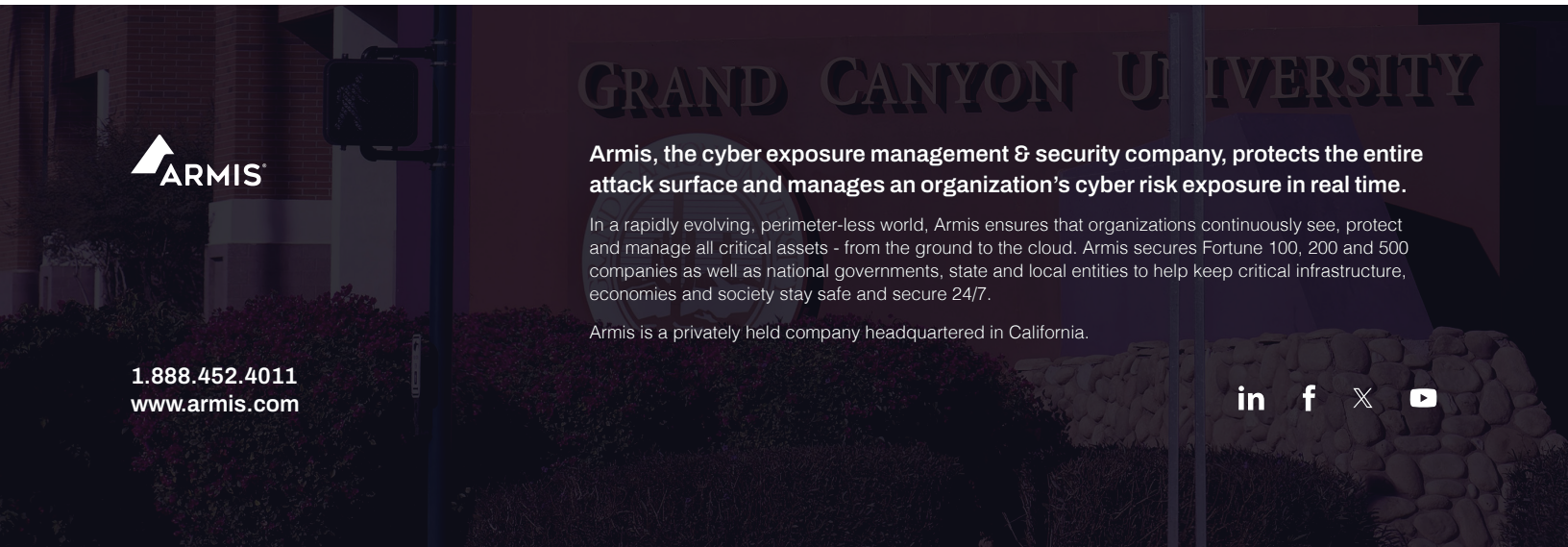
"Armis is the enforcement arm for what we want to happen in our environment and with our assets. Some of the most prominent results are in the realm of implementing agent compliance. Our former asset inventory management solution just wasn't cutting it, but Armis integrates asset data with all our other systems, giving us the full picture so we can bring every asset into compliance," said Manrod.

Additionally, Armis has promoted proactive security by continuously monitoring for unusual traffic patterns, system errors, and other vulnerabilities, accelerating the IT team's incident response time.

"Armis not only gives us a full picture of all our asset inventory, it also applies intelligence so we now discover issues through passive vulnerability detection," said IT Security Engineer Cameron Kownack. "Armis gives us direct vulnerability data from our environment that we can use in an actionable manner, from an internal-to-internal vantage point. Another huge win is identification of assets that use insecure protocols. Thanks to Armis, we've been able to resolve those issues."

Purple team testing is another area where Armis saves GCU significant time. "Armis gives us a single pane of glass and simple search queries for finding different paths to different areas of the environment, drastically hastening and simplifying the process," said Manrod. "I love doing augmented purple teaming with Armis."

"Armis is essential to our cybersecurity strategy because it's the enforcement arm that helps us decide what we want to happen in our environment and with our assets. Before Armis, we made policies, we checked, we scanned, and we hoped. With Armis, we know," Manrod concluded. "As we move forward, we plan to go deeper with Armis to chase down and resolve vulnerabilities in our environment."




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