CASE STUDY // TEXAS A&M

AXONIUS

HOW TEXAS A&M GAINED INSIGHT AND CLARITY WITH AXONIUS

THE AXONIUS PLATFORM

The state's first public institution of **higher learning**, Texas A&M University, opened its doors in 1876 and remains the largest public research-focused university in the United States with nearly 80,000 students.

TEXAS A&M UNIVERSITY

BALANCING ON A HIGH WIRE

With research-generated annual expenditures of more than $1.153B during FY22, there's a lot going on at Texas A&M University (TAMU). Whether students and researchers are cloning rare animals and plants or experimenting with rocket science, TAMU IT security and risk teams maintain a lot of confidential data and information that need to be kept secure.

Adam Mikeal, CISO, and Kyle Levenick, Program Director for the IT Security & Risk team at TAMU, lead their team to provide IT services to all faculty, staff, and students on campus and protect infrastructure against digital threats. They knew that previous IT infrastructure made it hard to grab real-time data and began uncovering coverage gaps in devices across the university. This complexity eventually led to

Employees

31,000+ faculty and staff

Key Challenges

- Creating and maintaining an accurate inventory of assets
- Gaining insight into enormous amounts of sensitive data
- Closing device security gaps across colleges

Solution

Axonius Cybersecurity Asset Management

Results

With Axonius, Texas A&M has a constant and consistent view of IT assets across nearly all verticals. The IT team has a better understanding of its architecture than ever before and can take proactive steps to mitigate issues, vulnerabilities, and problems.

> "As a research institution, we have every type of data. Literally. If there is a federal regulation around data, we have some of that data here."

Adam Mikeal
CISO, TEXAS A&M

Mikeal and Levenick feeling like they were balancing on a high wire.

That's when they started searching for a solution that would help them keep data up-to-date and close the gaps – before it was too late.

NAVIGATING THE CHALLENGES OF UNRELIABLE DATA

The breadth of research conducted on TAMU grounds results in almost every type of data existing in its infrastructure, which means that TAMU must stay compliant with virtually every type of regulatory framework. It operates a teaching hospital, so it must follow HIPAA regulations, conducts research under DoD regulations, and is also governed under International Traffic in Arms Regulations (ITAR), since federal weapons data research is conducted on campus. Beyond those regulations, the university is also regulated as a bank, since it grants financial loans to students.

All of this regulatory complexity meant that Mikeal and Levenick had to remain agile while managing data from what seemed like an endless amount of sources.

This ended up being a huge challenge. TAMU used a centralized financial asset management system. While it was largely accurate, almost all the data in this system was entered manually. This led to the possibility of errors and outdated data. The best case scenario was that data was only a few days old – but this also meant that the data could be unreliable or even months old.

As Mikeal and Levenick reviewed organizational device usage, they also started to find coverage gaps. In a university setting, there are tens of thousands of devices. But many of those may sit in a drawer for six months during the year because a faculty member isn't on campus during the summer, which creates even more complexity and confusion. Answering questions about what devices were being used and what software was on them became increasingly challenging – which isn't ideal during a security incident when finding answers to questions about usage is crucial.

You might think that the easiest way to control this sensitive information is by locking it down. But that's not possible when researchers at TAMU want to collaborate with peers at other institutions across the U.S. and across the globe. Many of the regulatory frameworks the university operates under require accurate inventories of resources, hardware, and software. That's why the IT department turned to Axonius.

GAINING VISIBILITY WITH AXONIUS

The team picked Axonius because they were struggling to gain a complete picture of their tech stack. Axonius Cybersecurity Asset Management provides visibility into the devices that are used within each college, giving IT leaders the ability to then keep those assets secure. Axonius also helps the university uncover accurate, reliable data that provides the context and information Mikeal and Levenick need to meet audit requirements. "Having the right data is what we really need to start making the right decisions," said Levenick. The IT team can now read data from any source and easily access it in one place – allowing them to merge groups, get read-only credentials, plug into their existing systems, and gain even more visibility.

Another reason Mikeal and Levenick chose Axonius is because they could now ask questions that were impossible to ask without a lot of manual stitching of data. Answers to questions like "what laptops are missing antivirus?" or "what devices need the latest Windows security update?" were now a quick query away. The team can also easily see what devices have been used recently and keep those devices secure. Mikeal and Levenick were excited to learn that the Axonius team can help make any adapters needed to ensure that the Axonius Platform integrates easily with whatever data sources university staff already plugged into – saving the IT team enormous amounts of time and unlocking even more data.

Using Axonius hasn't only been beneficial for the IT and security teams – the platform has increased efficiency for operational teams as well, who have similarly come to rely on the information Axonius provides. Dallas Ramsey, a security analyst at TAMU, collaborated with nearly every group across the university to build out customized operational dashboards for each function. Ramsey worked directly with colleagues to understand their specific needs and share how the Axonius Platform could help meet their individual goals.

> **" This was a light bulb moment where we realized we don't have to do this ourselves. We can just ask the Axonius team for help. This is incredible."**

Kyle Levenick
PROGRAM DIRECTOR FOR THE IT SECURITY & RISK TEAM, TEXAS A&M

Over the past year, the university has brought over 300 active users into the environment – 300 employees who are now able to look at their own data and ask the right questions about their devices. And with the help of Axonius, the answers they find are now accurate and help determine gaps in security. "We put a lot of power in the hands of our users to do what they need and want to do with the data," says Levenick.

The extended visibility gained by using Axonius has allowed teams to more accurately share information with university leadership. The Axonius Platform empowers TAMU employees to communicate what devices are out of date or missing software, information surrounding vulnerabilities, and exactly how the budget should be adjusted to meet IT needs. "We have a better understanding of 'what's out there' than ever before, and can take proactive steps to mitigate any issues, vulnerabilities, or problems."