AXONIUS

DCU Leverages Axonius to Increase Asset Visibility and Improve Security Control Coverage

DCU

Digital Federal Credit Union (DCU) is a not-for-profit, member-owned credit union that serves over 900,000 members and more than 700 organizations in all 50 states. DCU's services are wide-ranging, including business and consumer banking and lending, a full-service real estate agency, and robust insurance coverage.

EMPLOYEES
1,500

KEY CHALLENGES
Consolidating data scattered across multiple disparate systems to compile accurate security information and drive true visibility into asset protection.

SOLUTION
Axonius Cybersecurity Asset Management Platform

RESULTS
DCU centralized their systems using Axonius to see clear, actionable data – such as which devices needed protection – and address gaps as they were discovered.

Seeking Visibility Across Systems

DCU's cybersecurity team operates with a core belief: asset management is an integral part of every company's security framework. As Assistant Manager of Information Security Risk Management Mike Conroy put it, "Our security framework needs the 'what' and 'where' of all assets to be effective."

But network visibility can elude even the most dedicated teams. The DCU team was challenged to understand all of their systems since security asset data was being collected and analyzed from multiple, often siloed, systems. The process was slow and tedious.

As a result, DCU's team lacked insight into potential gaps in its security coverage. "You'd have multiple systems that know something about all your assets, like an antivirus – or at least what you thought was all your assets… It was tough to know whether or not everything was fully protected," Conroy explained.

Conroy and his team often discovered coverage gaps during routine maintenance, identifying assets not managed or tracked by any of DCU's multiple software programs.

Frustration grew around two central issues:
1. Lack of confidence in available data, particularly around security solution coverage
2. Continual discovery of assets lacking protection, often outside of normal policy, procedures, or management systems

## Finding a Solution for Security Risks

When the global pandemic hit in early 2020, DCU's workforce went fully remote. Suddenly, the team faced new challenges: with many assets now offsite, it became even harder to gain visibility into scattered devices.

Within a few months, DCU began the search for an asset management system.

Their criteria for a solution were simple – a platform that could:
- Integrate all of their data sources
- Consolidate that information and make it easily searchable

So when a DCU team member heard about Axonius on a podcast, the DCU team quickly scheduled an overview and a trial – then put together a business case. For Conroy, the case was clear. "We have all these different sources. They don't reconcile very easily. We can't do it manually. It's too much data. But this product takes all that information and does it for you with minimal overhead."
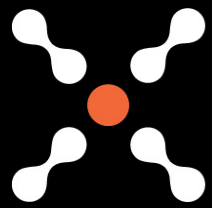
Axonius took what we thought we knew about our assets and gave us something a lot closer to the truth. It was able to take separate pieces of data, combine them together to reconcile that data, and really show us where our gaps were.

MIKE CONROY

ASSISTANT MANAGER OF INFORMATION
SECURITY RISK MANAGEMENT, DCU

Maximizing Asset Visibility and Security

By implementing Axonius – a platform designed for cybersecurity asset management – the DCU team was able to swiftly integrate its IT and security systems and view them in one central, searchable console.

In fact, the vast majority of DCU's security tech stack already had pre-built integrations in the Axonius adapter library. The Axonius team responded quickly to any requests for new programs and added them to the library.

The dashboard enabled unprecedented visibility and analysis with the confidence that any data used was being pulled from all of DCU's systems and across its environment. DCU's team soon gained a thorough understanding of their complete asset inventory, coverage gaps, and more.

Axonius then enabled the team to turn this data into concrete action, from enforcing policies to ensuring all assets were covered by security solutions, such as endpoint protection and vulnerability management solutions.

Gaining Visibility Into Security Data

Now, Axonius is vital to DCU's security environment. "Without Axonius, we wouldn't have had a full understanding of our asset data," Conroy said.

Where before, DCU had been limited by the accuracy of each individual solution, it could now correlate different sources of truth to gain insight into its environment and discover unprotected assets. This was a huge upgrade.

"If you don't have something pulling that all together for you, the best you can do is work with spreadsheets to pull all this data manually out of all the different systems. It would take you a month just to reconcile all that. [Axonius] does it for you every single night," Conroy said.

Since Axonius came on board, DCU has increased the number of protected remote devices by 18%. The cybersecurity team has also leveraged the platform's clean, simple dashboards to present program results back to their CISO and other DCU executives effectively. Ultimately, though, the support behind the platform has been just as key for Conroy and his team. "The number one benefit of working with Axonius is the vendor relationship … When you have something that you need or even something that you want, they are very receptive to it. They love putting in new features that their customers want."
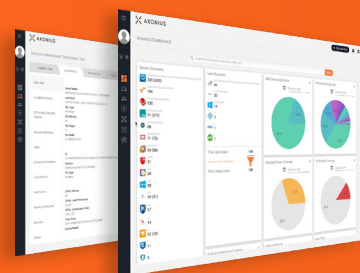
Experience the difference.

Axonius is the cybersecurity asset management platform that lets IT and security teams see devices for what they are, in order to manage and secure them all. **Interested in seeing what Axonius can do for your organization?**

LET'S TALK →