AXONIUS

CUSTOMER CASE STUDY

Global Enterprise Wacom Achieves Asset Management Clarity With Axonius

wacom

Wacom is the leading global manufacturer of pen tablets – including interactive pen displays and pen computers – for creative users. The company also provides digital solutions, from apps to a cutting-edge universal inking engine.

EMPLOYEES

1,000+

KEY CHALLENGES

Obtaining an accurate asset inventory that included Wacom's core systems, all its platforms, and users across any network.

SOLUTION

Axonius Cybersecurity Asset Management Platform

RESULTS

Wacom established true asset management visibility and a comprehensive inventory across its entire environment with Axonius. The cybersecurity team also leveraged the platform to enhance compliance validation, rogue device detection, correlation discovery, software project deployment, and more.

Seeking a Rich, Comprehensive Asset Inventory

Wacom's cybersecurity team knew that they were operating with limited information. In the past, their operations relied on a single scanning system that:

1. Wasn't agent-based
2. Didn't account for network location
3. Only queried active directory, not Wacom's other core identity management system

As a result, Wacom's asset inventory had significant gaps – and became more inaccurate as the company added more remote workers off its network. Moreover, their scanning tool didn't have any flexibility regarding DPA/MSA.

Their Cybersecurity and Incident Response Director, Mark Priess, summed it up: "We needed a system that was more flexible, would reach into other platforms, and would provide us with a more comprehensive assessment of our host and user assets... If you don't know what you have, it's very hard to choose security tools and develop policies."

Upgrading to a Flexible, Powerful Tool

To achieve that comprehensive inventory, Wacom needed a new system to replace its existing scanning tool. As Priess put it, "An asset management tool that accurately identifies active systems, related users and system owners is essential to success. I believe you can look at a company's asset management capability and tell right there how effective their overall program will be."

Priess researched cybersecurity tools that would provide "more flexibility, functionality, and ability to adapt to [Wacom's] infrastructure as it evolved."

He soon found Axonius, which met all those criteria from the start and was the only tool on the market that could tie into all of Wacom's core systems. Priess also appreciated that during the demo, the Axonius engineering and development teams collaborated quickly and smoothly to customize the platform for Wacom's needs.

“Axonius enabled clarity with regards to asset management, assurance of coverage, and the discovery of previously unknown correlations.

MARK PRIESS
DIRECTOR, CYBERSECURITY & INCIDENT RESPONSE

The Right Capabilities With Axonius

Axonius stood out as the ideal cybersecurity asset management solution for Wacom primarily because of its near-limitless integration capabilities. Priess noted, “I’m not aware of another tool that has as many integrations with other platforms... The responsiveness from the engineering team to add new integrations is another differentiator.”

With Axonius, the Wacom cybersecurity team could retrieve asset and user information from not just all their core systems, but also any system that they worked with, no matter how small. The platform provided exactly what they sought: **a single source of truth for all activity, users, devices, and their respective correlations** – despite network growth, system change, or user turnover.

Axonius delivered another key functionality for the Wacom team: improved correlation and data reporting. Priess said, “We wanted to be able to create reports that showed which systems were active, when they were seen last, what tools saw them and which ones didn’t, and so on.” Axonius made that possible.

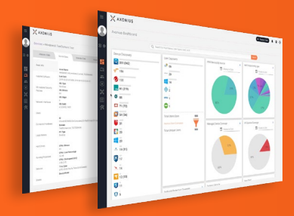
Accomplishing Key Asset Management Victories

Now, Wacom has full visibility into all of its core systems via a single platform: Axonius. They currently pull feeds from 17 different sources to see which devices are managed by which systems and identify any gaps, all while saving time on manual verifications.

Priess says this has enabled them to achieve true asset management clarity, which he sees as vital: “Users and assets are where the data resides, and data is the centerpoint of cybersecurity protection. The whole point is to protect data from loss or alteration. The best way to start along that path is to ensure you know where it all is. That starts with asset management.”

This visibility has led to other benefits. Because Axonius scans all systems, Wacom uses it to validate compliance and coverage, detect rogue devices, and discover previously unknown correlations. Axonius also helps Wacom’s team implement IT projects that are based on device/user associations, as well as monitor software deployments via integrations with multiple apps and systems instead of relying on a single source.

For Priess, Axonius was the perfect solution for Wacom’s needs. “I’d recommend Axonius to anyone who needs to customize their asset management tool to fit their business needs and not the other way around.”



Experience it yourself.

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 →