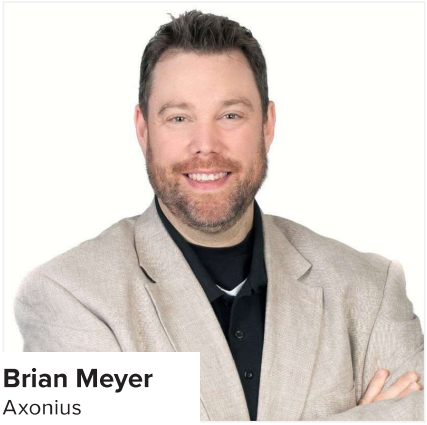
AXONIUS

Keeping blind spots from becoming vulnerabilities

Cybersecurity asset management streamlines a complex arsenal of tools and strengthens the enforcement of security policies



Brian Meyer
Axonius

> "VISIBILITY IS THE FOUNDATION OF MODERN CYBERSECURITY FRAMEWORKS, INCLUDING ZERO TRUST. FAR FROM BEING OPTIONAL, IT'S THE PREREQUISITE FOR EVERY OTHER SECURITY CONTROL."

Agencies operate in increasingly complex environments, and without full visibility into cloud-based, on-premises and internet of things systems, blind spots can quickly become vulnerabilities. For government agencies, this isn't just about compliance—it's about mission assurance. A single unmanaged asset can be the entry point for a breach that disrupts critical services. Furthermore, visibility is the foundation of modern cybersecurity frameworks, including zero trust. Far from being optional, it's the prerequisite for every other security control.

Unfortunately, despite all their dashboards and tools, many agencies don't have the visibility they think they have. Large organizations might use dozens of security tools, and every tool has a different approach to navigation and a different language to learn. When users struggle to understand the tools, they often resort to dumping asset details into a spreadsheet and then try to correlate the data to identify security gaps. It takes a lot of manpower to generate those reports, but the information is outdated as soon as it is exported.

A common landscape across all business units

When dozens of security tools are each generating data in silos, the results are complexity and operational fatigue. The solution isn't to add more tools; it's to make existing tools work together. Cybersecurity asset management is the key to that orchestration. It acts as the connective tissue by aggregating data from all the tools, normalizing it and giving teams a single source of truth. That means policies can be enforced consistently across the IT environment.

The Axonius cybersecurity asset management platform is the first solution in the global market that connects all of an organization's cybersecurity and operational technologies to generate a single, comprehensive record of the devices on that network. It creates a common landscape across business units and pulls together information in an easily readable format.

For example, our platform allows the compliance team to see all the devices that endpoint security doesn't know about and understand the various reasons why those devices aren't known. Then the compliance experts can work proactively with their operations counterparts to close the security gaps.

The way to eliminate uncertainty

The blind spots that Axonius reveals often take customers by surprise. The most successful agencies are the ones that embrace the opportunity to improve and treat their vendors as partners so they can take full advantage of the industry's best practices to close their security gaps.

A real-world example of our platform's effectiveness is its integration into the Cybersecurity and Infrastructure Security

Agency's Continuous Diagnostics and Mitigation program. For the past five years, Axonius has played a dominant role in automating activities in all six groups in CDM's framework for improving the security of federal civilian networks. Because of that success, Axonius is now officially part of the CDM pipeline, and CISA is deploying our platform across CDM to automate what its team has been doing manually for the past 10 years.

Many agencies are stuck in reactive mode, responding to alerts after the fact. Axonius flips that by giving teams the context they need to identify gaps before they become incidents. With our platform, agencies can automatically validate security controls, detect unmanaged devices and ensure compliance continuously, not just during audits. Being proactive isn't about predicting the future—it's about eliminating uncertainty. Axonius gives agencies the confidence that their security posture matches their policies every day. ■

Brian "Stretch" Meyer *is federal field CTO at Axonius Federal.*

ADOBE STOCK // WAFIQ