Building the Business Case for *Cybersecurity Asset Management*

The Growing Digital Landscape

The modern enterprise is a sprawling digital ecosystem. On-premises servers, remote devices, cloud workloads, SaaS applications, and an ever-expanding web of user identities. While this digital sprawl fuels business innovation, it also creates a tangled mess of security risks. With so many assets scattered across multiple environments, IT and security teams are left struggling to answer the simplest of questions:

- What assets do we actually have?
- Where are they located?
- Who has access to them?
- How does this affect my engineers across multiple teams?
- How can I confidently report our risk to the Board?

Attackers Are Moving Faster than Security Teams

Cyber criminals thrive in chaos, exploiting visibility gaps and misconfigurations to infiltrate organizations. And they're succeeding. Ransomware attacks, supply chain breaches, and insider threats are growing at an alarming pace. Meanwhile, security teams are trying to keep up, drowning in disparate security tools, siloed asset data, and manual processes.

Organizations often deploy multiple asset management tools, each providing a fraction of the overall picture. The result? A fragmented view that makes it nearly impossible to enforce security policies or detect threats before it's too late.

> "Simply put, if you don't know about an asset, you can't protect it."

Doug Graham
Chief Trust Officer, Lionbridge

The Illusion of Control

Many organizations believe they have a handle on their cybersecurity posture because they have robust security stacks in place. A false sense of security can be just as dangerous as having none at all. Without a comprehensive asset inventory and its relationship in my environment, security teams lack the foundation they need to:

- Quickly detect unprotected or misconfigured critical assets
- Enforce security policies across all assets
- Effectively prioritize vulnerabilities and risk mitigation efforts
- Ensure compliance with regulatory mandates and frameworks

Risks of Inaction: The True Cost of an Inaccurate Cyber Inventory

The stakes have never been higher. When organizations fail to establish a comprehensive cybersecurity asset management strategy, they risk:

Data breaches and cyberattacks: The average data breach costs nearly $5 million, according to IBM's 2024 Cost of a Data Breach report.

Regulatory fines and compliance failures: Non-compliance with mandates like PCI DSS 4.0, HIPAA 2023, GDPR, and the new NIST Cybersecurity Framework 2.0 framework can result in massive penalties.

Team inefficiencies: Security teams waste countless hours manually gathering asset data, slowing down incident response and increasing MTTR (Mean Time to Respond).

Software deployment gaps: Organizations often purchase security tools that aren't fully deployed, leaving assets unprotected and wasting valuable budget.

"Axonius has given us visibility that previously required taking multiple outputs from different sources and correlating them to get a clean result. *They greatly reduced the time* we would have spent, and increased our accuracy."

Steve Kjaer
CISO, Poly

The Disparate Tool Nightmare

Security teams are already stretched thin. According to a 2023 (ISC)² Cybersecurity Workforce Study, the global cybersecurity workforce gap has reached 3.4 million professionals. Without automation and visibility, teams are left playing an endless game of catch-up, manually stitching together asset data from disparate sources.

Managing cybersecurity assets using multiple, disconnected tools creates unnecessary complexity. Traditional methods often involve:

- **Spreadsheets and manual audits:** Time-consuming and error-prone
- **CMDBs (Configuration Management Databases):** Require constant updates and don't provide real-time security insights
- **Multiple security platforms:** Each with its own valuable dataset, but siloed and leading to blind spots and inconsistent security enforcement. Also, gaining the full value from that tool and its data.

When security solutions fail to provide a unified view, attackers exploit the gaps. Security teams can't protect what they can't see.

Comprehensive Cybersecurity Asset Management

To combat escalating threats and complexity, organizations need a cybersecurity asset management solution that provides:

A complete, up-to-date asset inventory: Every device, cloud instance, SaaS application, and user identity in a single, unified view.

Security posture validation: Automatically enforce security policies, ensuring assets are properly configured and protected.

Automated remediation: Reduce the attack surface by automatically triggering security actions when risks are detected.

Context-rich insights: Correlate asset data from multiple sources to improve decision-making.

Agentless and Scannerless deployment: Deploying additional agents and scanners is time-consuming and often leaves wide gaps in your asset inventory.

> "This combination of features makes Axonius a powerful tool for improving asset management and our overall security posture. Axonius is now one of our foundational pillars for all our security programs."
>
> Ingram Micro Security Team

> "You can have *a lot of disparate systems managed by disparate teams,* and it can be hard to gain a comprehensive view of what's on your network."
>
> Jason Loomis
> CISO, Mindbody

The Axonius *Approach*

A world-class cybersecurity asset management solution like Axonius aggregates, normalizes, deduplicates, and correlates asset data from existing data sources to:

- Eliminate asset blind spots by integrating with 1,200+ IT, security, and business data sources
- Identify and close security gaps by continuously monitoring asset compliance
- Automate policy enforcement by triggering security actions when deviations occur
- Simplify security operations by reducing manual effort and improving incident response times
- Reduce time and complexity, as well as asset gaps, with an agentless architecture

"Axonius reduced the time it takes to find asset information from *30 to 60 minutes to under 30 seconds.* It has been a huge efficiency win. It also shines light on dark places in the environment where asset repositories may have gotten cluttered and where assets may be missing a bulk of the tooling you'd expect to see."

Gartner Peer Review

Use Case: Vulnerability Management

Your Vulnerability Scanner Has a Blind Spot. Axonius Gives It X-Ray Vision.

Vulnerability assessment tools are great, when they know what to scan. But what about the devices hiding in the shadows? Virtual machines, cloud instances, and other assets often slip through the cracks, leaving security gaps wide open. Sure, you could check your VA scanner's admin console, but that only shows what's already being scanned, not what's missing. And guessing isn't a solid security strategy.

That's where Axonius comes in. By aggregating and correlating data from your VA scanner, network, IAM solutions, and cloud infrastructure, Axonius reveals which devices are flying under the radar and missing from your VA scan schedule. We also provide robust information regarding context, along with valuable enrichment (EPSS, CISA, NVD, etc.), detailed reports, and the ability to provide transparency across business units.

Better yet, Axonius lets you group assets by subnet, VLAN, OS, ownership, and more, so you can prioritize vulnerability management and patching like a pro. No more blind spots. No more security surprises. Just complete asset visibility.

By running simple queries in the Axonius Query Wizard, your IT and security teams can identify all devices running applications that may be affected by vulnerabilities. Even better, the Axonius Security Policy Enforcement Center lets you trigger automated action. As an example, you can create an incident and alert asset owners so they can take immediate action to patch.

Use Case: Security Solution Development

Your Security Tools Can't Protect What They Can't See. Axonius Fixes That

Companies invest heavily in security tools, only to later realize they're not actually deployed everywhere. It's like buying locks for your doors/windows and forgetting to install some of them on your front windows. Axonius helps recoup that lost value by continuously surfacing devices missing critical agents and software, ensuring no assets are left unprotected. When we find gaps, we automatically alert the right team to take action.

One of the most common challenges? Finding devices missing endpoint agents. Sure, your agent's admin console shows covered devices, but what about the ones slipping through the cracks? With the Axonius Query Wizard, you can instantly pinpoint devices missing essential endpoint agents, whether it's a simple "show me everything without an agent" or a granular search for OS-specific EDR and EPP gaps. No more security blind spots. No more wasted investments. Just full visibility and control.

Use Case: Incident Response Investigations

Incident Response Shouldn't Feel Like a Treasure Hunt. Axonius Makes It Easy.

Security alerts tell you what happened, but not always where or who's involved. That leaves security analysts scrambling to track down devices linked to an incident, wasting precious time. Axonius eliminates the guesswork by providing a single source of truth for all assets, speeding up alert triage and incident response. With historical data, analysts can match asset attributes to the exact moment of compromise.

By connecting rich data from multiple sources, including devices, users, and cloud assets, Axonius helps answer critical questions instantly, such as:

- Which devices and users are involved?
- Where are they located?
- What software is running on them?

Need to take action? Just query any IP from an alert in Axonius to notify teams, trigger enforcement actions, or even isolate impacted devices and users. No wild goose chases required.

Use Case: Empower IT Operations

Axonius for IT Ops: Less Guesswork, More Control

IT teams need real-time visibility, but keeping up with constant changes is like herding digital cats. Axonius makes it easy by continuously surfacing conditions across your IT environment, tracking changes over time, and putting all the right data in one place.

Here's how Axonius helps IT operations teams work smarter, not harder:

- **Supercharges Your CMDB:** No more manual updates. Axonius auto-populates your CMDB with fully correlated asset data, saving time and effort.
- **Ensures Proper Server Configurations:** Whether Windows or Linux, Axonius keeps tabs on configurations, ensuring servers are up-to-date and covered by the right security controls.
- **Monitors User Access & Permissions:** Aggregating data from IAM, directory services, and remote work tools, Axonius helps track user access and permission changes, so nothing slips through the cracks.

No more chasing data across multiple systems. With Axonius, IT Ops finally gains the visibility and control they need, without the headaches.

"Axonious enabled us to conduct a fully robust investigation, quite literally in one place. *It's incredibly easy to build a user profile when an investigation comes up.* That means investigation across any board, whether that's incident response or vulnerability management. I think very few solutions are able to provide something like this."

Andrea Youwakim
Security Analyst, Avant

Business Benefits

By implementing the right cybersecurity asset management solution, organizations can achieve:

Significant time savings: Automating asset inventory processes reduces manual workloads and allows teams to focus on high-value tasks.

Stronger security posture: A complete and up-to-date asset inventory reduces the likelihood of misconfigurations and security gaps.

Reduced compliance risks: Streamlined tracking and monitoring of in-scope assets ensures continuous compliance with regulatory requirements.

Optimized security investments: Ensure security tools are deployed effectively and are protecting all assets as intended.

Conclusion

Accurate cybersecurity asset management is no longer optional. It's a fundamental requirement for any organization looking to secure its digital infrastructure, optimize security operations, and reduce risk. By aggregating and correlating asset data from multiple sources, organizations gain the visibility and automation needed to protect against evolving cyber threats.