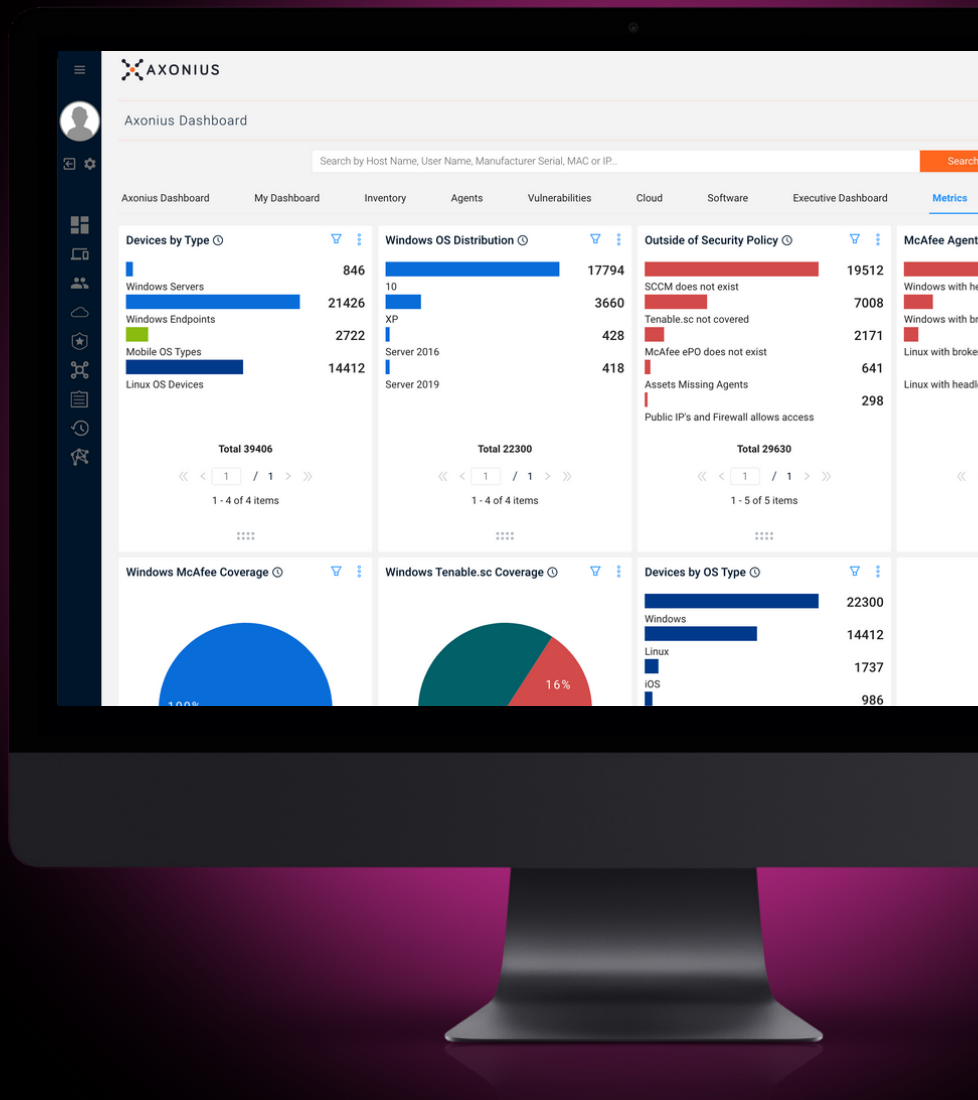
AXONIUS FOR CISOS

WHY CISOS TRUST AXONIUS

Chief Information Security Officers face an increasingly difficult set of responsibilities. They need **clear visibility** into their technology environment, yet information is spread across disparate tools and data sources. They have to implement and ensure policies that **minimize risk** and deploy security controls — while coordinating scarce and valuable resources that are often overwhelmed and reactive.



THE VISIBILITY BREADTH AND DEPTH CISOS NEED

That's why CISOs trust Axonius to start all security initiatives with a **comprehensive** understanding of the intersection of devices, cloud instances, SaaS applications, users — and the controls and solutions meant to secure and manage them.

There's no shortage of asset data. The challenge is separating the actionable, meaningful information from the noise. CISOs use Axonius dashboards and reports to understand security posture trends, prioritize action, and measure progress.

Key Benefits

REDUCE RISK

Cyber risk reduction is key to successful business operations. Axonius provides a clear understanding of all digital assets and their security posture so that CISOs can set the strategy for systematically managing vulnerabilities and asset-related risks across the organization.

SAVE TIME

No more manual accounting for assets. No more spreadsheets. No more manual data correlation. Axonius aggregates, normalizes, and correlates asset data from all deployed tools in the enterprise environment automatically and supplies a single PoV of the technology environment.

SIMPLIFY

Most organizations' infrastructures are so complex that crafting a comprehensive-yet-clear executive-level report is nearly impossible. Axonius simplifies cyber asset and cyber risk reporting by providing a unified view of the asset environment, all related risks, and progress against remediation.

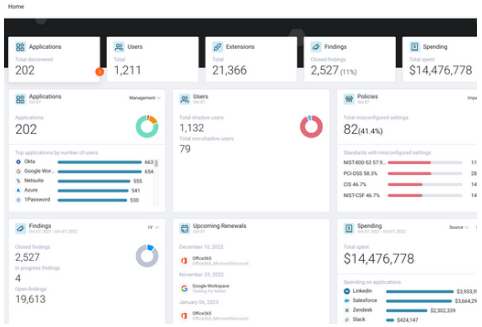
Use Cases

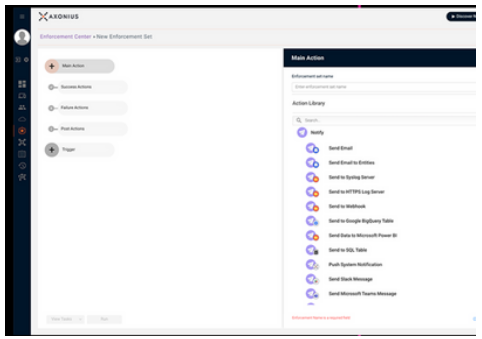
CYBER ASSET ATTACK SURFACE MANAGEMENT

- Axonius leverages API integrations with existing tools to provide a consolidated view of all assets, including SaaS apps.
- The Axonius correlation engine provides data on all deployed assets and missing controls for better vulnerability management.
- Instantly address attack surface threats by executing automated enforcement actions directly from the Axonius console.

VULNERABILITY MANAGEMENT

- Discover, track, prioritize, remediate, and report on all vulnerabilities across assets in your environment.
- Axonius identifies known vulnerabilities, maps them directly to assets, provides enrichment from third-party sources, and offers full context so security teams can prioritize remediation and make strategic decisions that make the organization more secure.





AXONIUS

Interested in seeing what Axonius can do for your organization?

LET'S TALK

> ***"The sheer excitement my team feels to have visibility into what's in our environment and to have it all in one location — I can't express how important that is for us."***
>
> **JASON LOOMIS**
> CISO, MINDBODY

How it Works

1. VISIBILITY

Gain a comprehensive asset inventory through an ecosystem of over 500 API integrations. Axonius collects data from all deployed assets then aggregates, normalizes, deduplicates, and correlates asset data to provide visibility into the network environment.

2. CONTROL

Uncover gaps in security policies, configurations, and hygiene. Axonius collects information about the security state of each asset to help security practitioners manage risk.

3. ENFORCE POLICY

Automaticallty apply security policies to reduce system weaknesses and harden assets against attack.