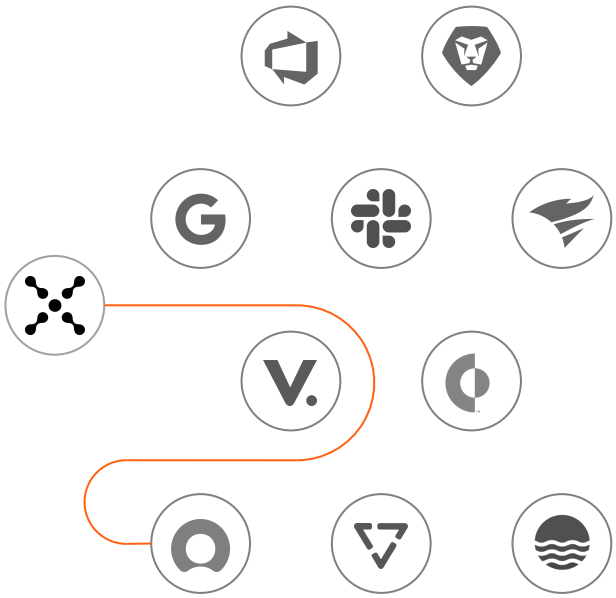
Axonius

Axonius Security for AI

Discover every AI asset, who owns it, and what it can access, then govern it confidently.



AI is a new asset class. Most security stacks only see fragments of it.

AI is spreading faster than security teams can review it. Employees adopt new tools on their own, vendors switch on AI features by default, and agents pick up access no one approved. Most teams can't answer basic questions: which AI tools are in use, which identities they run as, and what data they can reach. Without those answers, policies can't be enforced precisely. Teams end up choosing between blocking AI outright and accepting risk they can't measure.

Axonius closes that gap. By correlating data from across endpoints, web apps, cloud containers, and identity systems, Axonius builds one continuously updated inventory of every AI asset, from unsanctioned models and deployed agents to non-human identities and AI-enabled SaaS. Security teams get a complete view of AI usage and access, so they can govern it with precision instead of guesswork.

01

Complete AI inventory in days, with no new infrastructure

02

Identity-level visibility into every AI asset and its access

03

Policy enforcement at scale, without blanket bans

"Axonius provides us with a single source of visibility and a single source of truth. We're no longer arguing about what's there and what's not there, what's been patched and what's not been patched, and what coverage looks like."

Doug Graham, VP of Security, Lionbridge

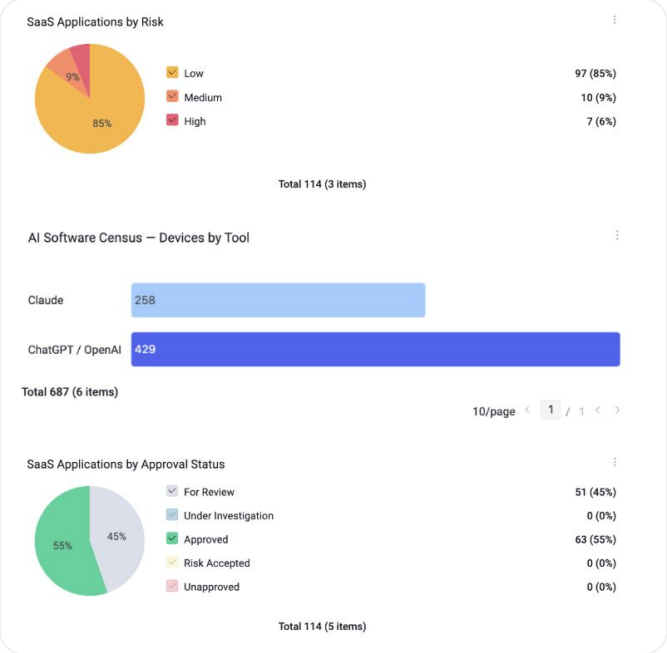
Axonius

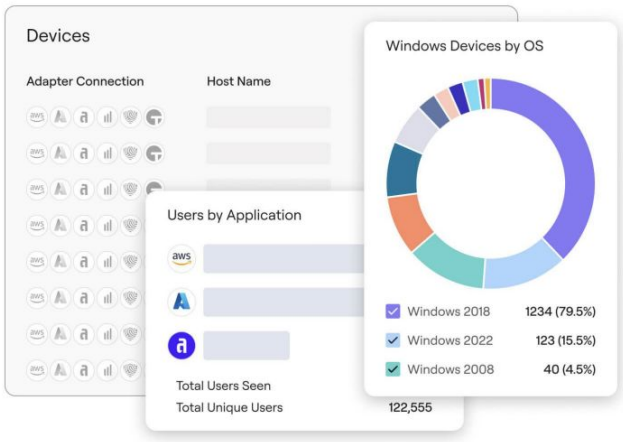
SHADOW AI DISCOVERY

Shadow AI doesn't announce itself. It accumulates.

Shadow AI hides in approved tools, unsanctioned apps, and internal builds. Each carries a different risk.

Axonius connects to more than 200 applications and classifies each as AI-native, AI-enhanced, or AI infrastructure. It also shows opt-in policies, where its models are trained, and the level of autonomy of the AI features. From day one, you know exactly what to sanction, restrict, or investigate.





AI ASSET INTELLIGENCE

An AI inventory built from data you already have

Your security tools already see pieces of your AI footprint. Axonius connects and correlates them to reveal installed AI tools, AI features enabled in your apps, ownerless agents with credentials, and unsanctioned model usage tied to real identities.

The result is one complete picture of what AI exists, who operates it, and what it can reach.

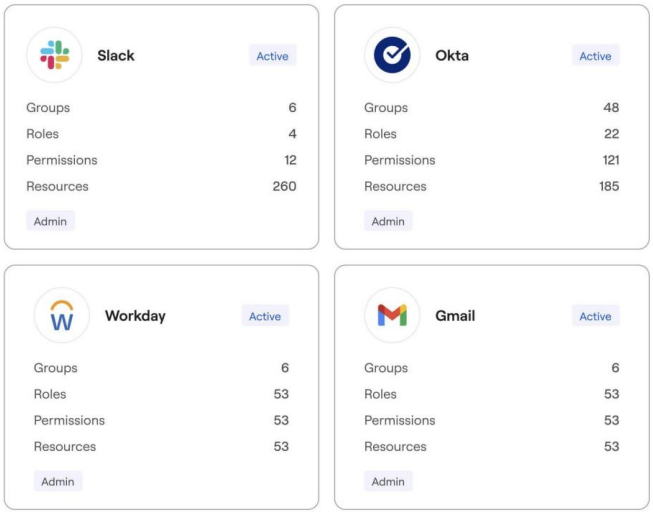
Axonius

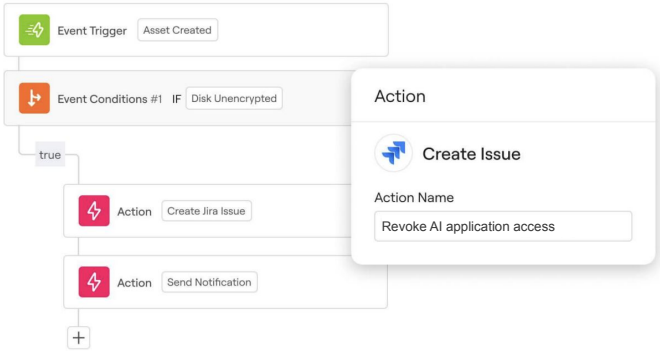
IDENTITY AND OWNERSHIP

Know who and what is behind every AI asset

Identity-to-asset mapping. Tie every AI asset to the identity it runs as, the permissions it holds, and the data it can reach.reach.

Non-human identity detection. Spot the agents and service accounts operating AI across your environment, including those with credentials but no owner.





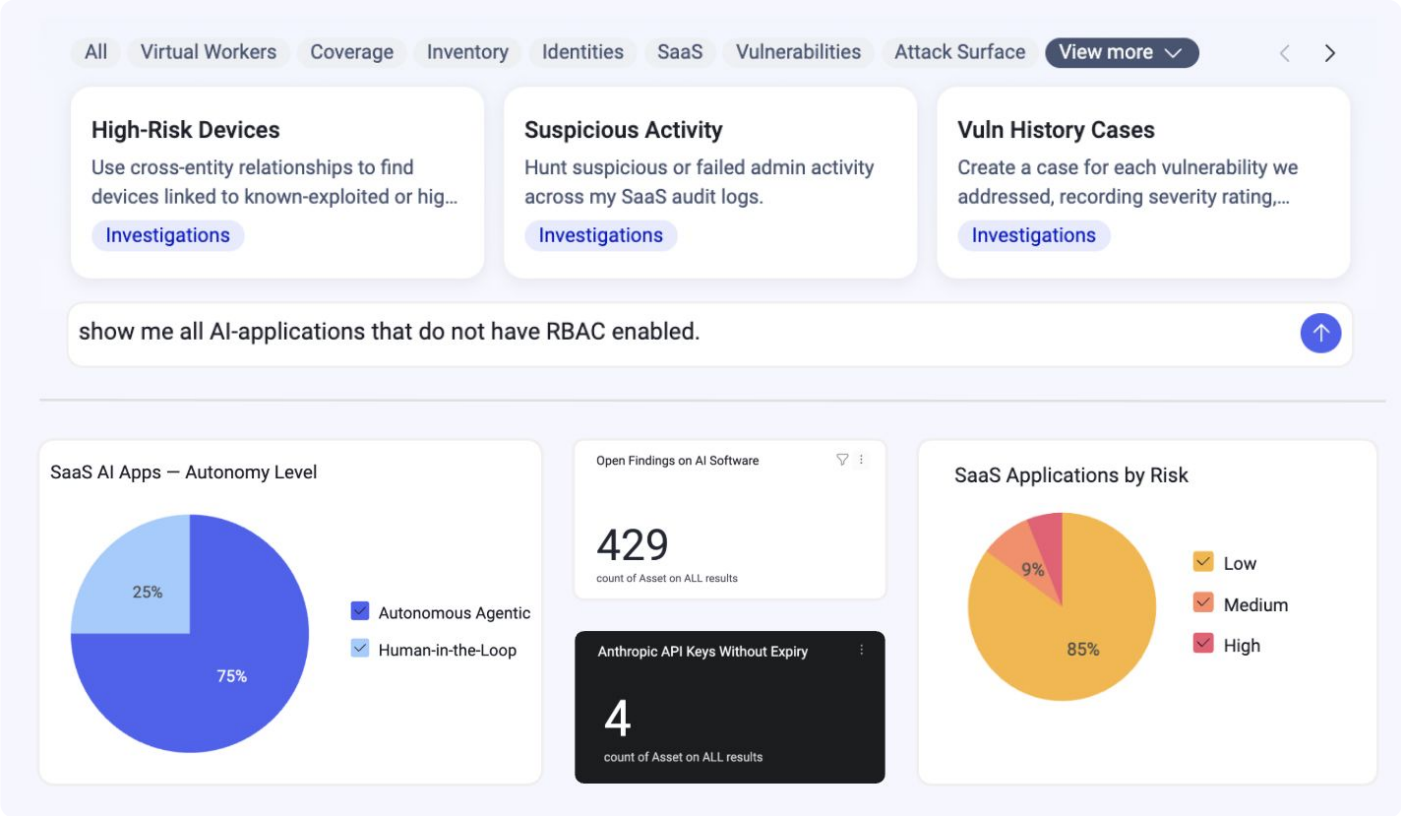
FROM VISIBILITY TO ACTION

Turn AI findings into automated response

Visibility is only the start. Axonius turns AI findings into action, automatically flagging over-permissioned agents and policy violations, routing them to the right owner, and remediating through Action Center.

With AI Companion and AI Workforce, teams can investigate findings faster and automate response at scale, closing gaps without blocking AI across the board.

You can't govern AI you can't see.



Establish and maintain AI posture

Security for AI runs on the Axonius Asset Cloud, the same reconciliation layer that security teams at Gigamon, TransUnion, Lionbridge, and hundreds of other organizations use today. AI assets aren't a separate module. They're a new asset class, correlated against the devices, identities, and exposures you already track, so AI risk is never assessed in isolation.

51%
more assets found than customers expected

87.5%
fewer unmanaged assets (from 20% to 2.5%)

86%
fewer tools per investigation (from 7 to 1)

Axonius

Request a demo