Axonius
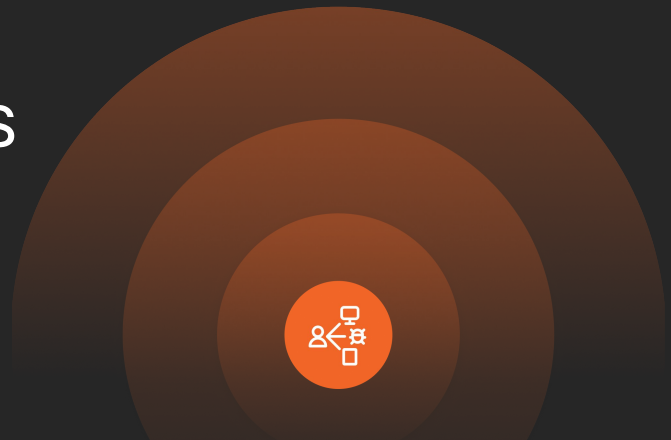
Axonius Cyber Assets

Step up from a static asset inventory to dynamic asset intelligence

Every security program starts with knowing what exists – but that's not where it ends. In dynamic environments, assets are in constant flux, and visibility alone isn't enough. Security teams need the ability to act with confidence and precision.

Axonius Cyber Assets provides a complete, accurate, and always up-to-date model of every asset across cloud, on-prem, SaaS, and hybrid environments. By aggregating and correlating data from thousands of systems and applications, Axonius turns fragmented asset data into a powerful foundation for action – enabling teams to uncover gaps, enforce policies, validate controls, and reduce risk at scale.

Axonius empowers intelligent action:

- **Continuous Asset Discovery**
  Correlate data from every tool to eliminate blind spots across your entire environment.

- **Contextual Risk Assessment**
  Unify asset profiles and relationships – vulnerabilities, users, software, configurations, and more – in one place.

- **Smart Prioritization Model**
  Identify gaps that actually matter based on exploitability, business impact, and control coverage.

- **Streamlined Mitigation Flows**
  Orchestrate actions across systems to enforce policy, remediate issues, and eliminate manual effort.

- **Program-Level Reporting**
  Get unified, cross-domain visibility to measure remediation, prove compliance, and track total posture.

Gain Total Attack Surface Visibility
See everything in one place. Axonius eliminates the guesswork by unifying all asset data into a single, comprehensive view that security teams can trust and act on.

Get Truthful Asset Intelligence
Raw asset data alone isn't enough. Axonius goes the extra mile to surface what's out of policy, at risk, or out of date – providing the ground truth for audits and investigations.

Drive Intelligent Action
Axonius doesn't stop at insight. We empower teams to orchestrate enforcement, automate fixes, and continuously validate outcomes.

> "
> Asset visibility is foundational to a security program — security teams need to know what assets exist in their environment and where those assets reside.

GARTNER: Emerging Tech: Evolving CAASM Beyond Cyber Asset Management

Axonius

Make actionable sense of your asset data

Axonius eliminates the guesswork of asset inventory by delivering a single, trusted view of your entire technology environment. No more reconciling spreadsheets, bouncing between tools, or chasing down owners.

Behind the scenes, Axonius integrates with thousands of data sources to continuously aggregate, normalize, deduplicate, and enrich asset records – ensuring every device, user, application, and workload is accounted for and accurate in real time.
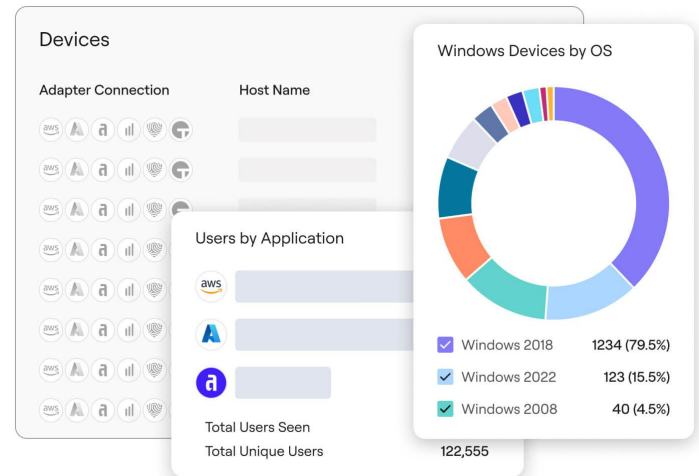
SMART ASSET INTELLIGENCE

Get blazing fast answers without the guesswork

Knowing what you have is just the start – Axonius shows you what's out of policy, out of date, or just plain risky. Whether you're chasing down misconfigurations, missing agents, or dormant accounts, you'll get answers in seconds.

By unifying asset metadata into a powerful queryable model, Axonius surfaces critical gaps like weak controls, configuration drift, and coverage blind spots – so teams can assess risk without wading through noise or incomplete data.
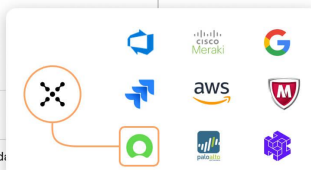
See the whole attack surface, not just the parts

Understanding risk requires more than lists and filters. Axonius shows you how assets connect, where risk propagates, and how to act with full context – with rich visuals.

The platform builds a relational map across users, devices, software, roles, and entitlements, so teams can visualize dependencies and take faster, more informed actions across threat response, hygiene optimization, and access validation.

Adhere to policies continuously
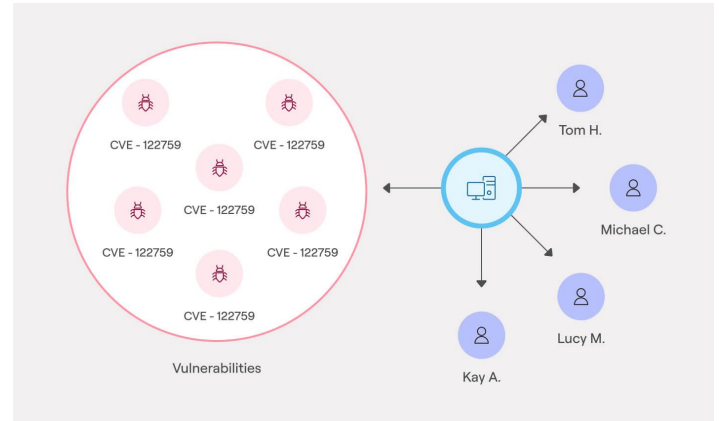
Axonius doesn't just reveal issues – we give you the power to fix them. From remediation to policy enforcement, the platform turns insight into action across your entire environment.

Through deep integrations with existing IT and security tools, Axonius automates the tasks that bog teams down – revoking access, closing vulnerabilities, updating configurations, or triggering custom workflows – all from a single control plane.
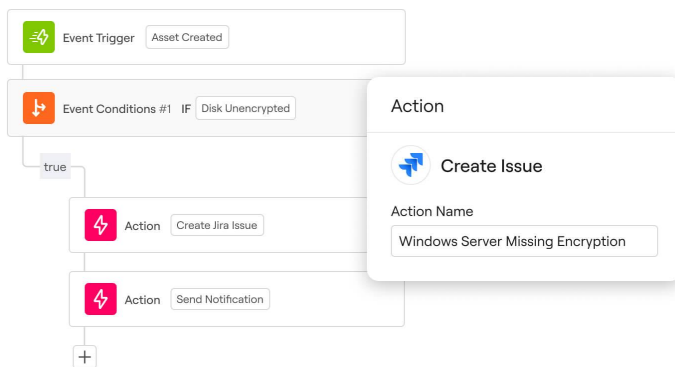
Key Capabilities

Axonius brings **actionability** to IT and Security teams by unifying cyber asset data across all environments, enriched with deep context and extended with powerful orchestration abilities.

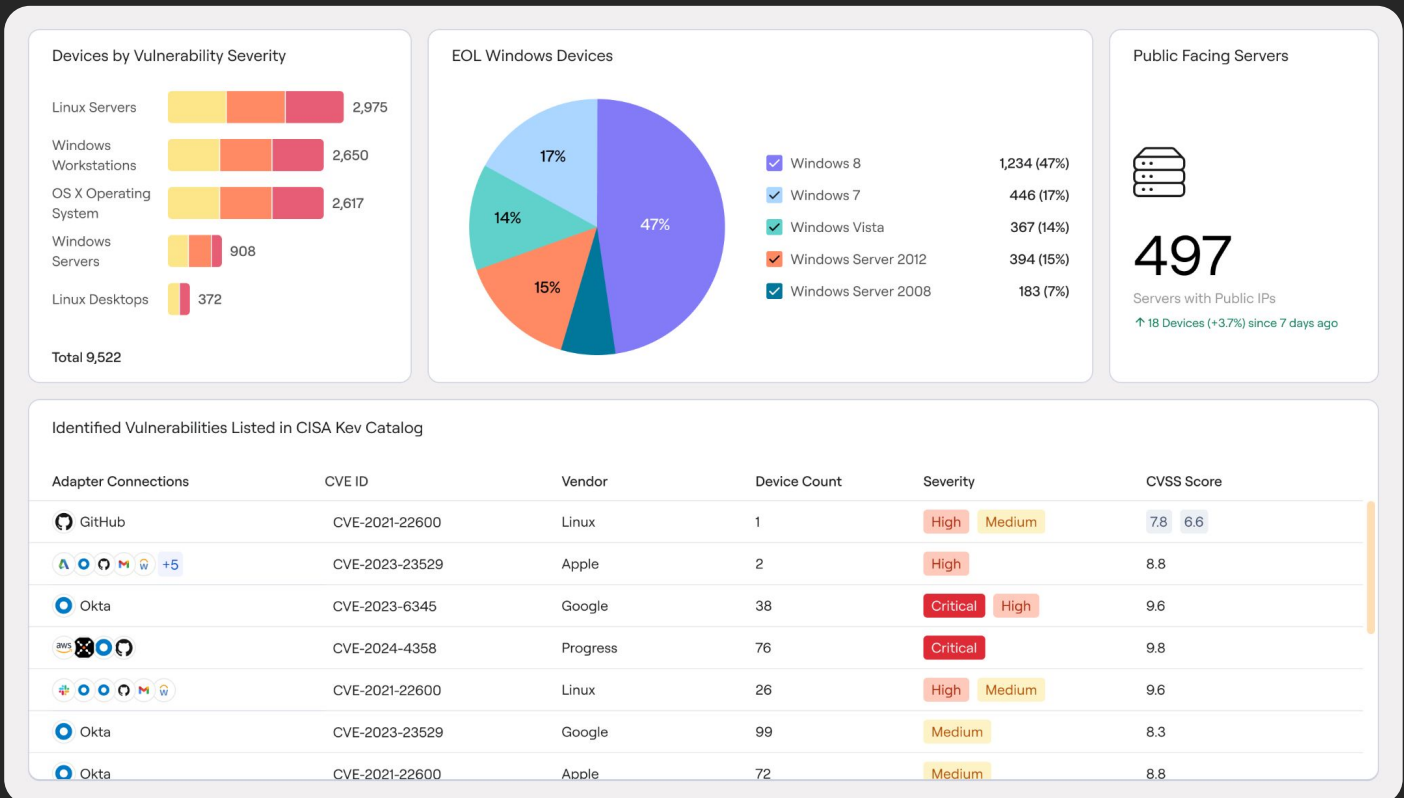| Feature	The Axonius approach
Unified Cyber Asset Catalog	Continuously aggregates and correlates assets from all environments into a single, searchable inventory
Enriched Asset Profiles	Combines data from multiple sources to provide deep context on every asset – users, software, risk, and more
Natural Language Search	Ask questions in plain English and get accurate results powered by the underlying asset model
Structured Query Builder	Build precise, multi-condition queries with ease to identify gaps, misconfigurations, or policy violations
Flexible Cyber Asset Dashboards	Visualize trends, metrics, and KPIs with customizable dashboards built for IT and Security stakeholders
Asset Graph	Visualizes relationships between assets – devices, users, apps, and more - to surface hidden connections and risks
Security Findings Center	Consolidates and correlates findings from multiple tools to give a unified view of risk across the environment
Data Analytics	Analyze query results over time to uncover trends, track changes, and support data-driven decisions
Automated Enforcement Actions	Trigger direct actions – like managing services, adding tags, or opening tickets – based on rules or on-demand
Asset Management Workflows	Automate multi-step processes across tools and teams to standardize responses and reduce manual effort
Case Management	Track, assign, and resolve issues in-platform with full context, audit history, and customizable fields
Fine-Grained Authorization	Control access by user role, asset type, or data source to enforce least privilege across teams

Axonius

Axonius

Take *action* with Axonius Cyber Assets

Devices by Vulnerability Severity

Linux Servers	2,975
Windows Workstations	2,650
OS X Operating System	2,617
Windows Servers	908
Linux Desktops	372

Total 9,522

EOL Windows Devices

☑	Windows 8	1,234 (47%)
☑	Windows 7	446 (17%)
☑	Windows Vista	367 (14%)
☑	Windows Server 2012	394 (15%)
☑	Windows Server 2008	183 (7%)

47% · 17% · 14% · 15%

Public Facing Servers

497

Servers with Public IPs

↑ 18 Devices (+3.7%) since 7 days ago

Identified Vulnerabilities Listed in CISA Kev Catalog

Adapter Connections	CVE ID	Vendor	Device Count	Severity	CVSS Score
GitHub	CVE-2021-22600	Linux	1	High Medium	7.8 6.6
⬤⬤⬤ M ⬤ +5	CVE-2023-23529	Apple	2	High	8.8
Okta	CVE-2023-6345	Google	38	Critical High	9.6
aws ⬤⬤⬤	CVE-2024-4358	Progress	76	Critical	9.8
⬤⬤⬤ M ⬤	CVE-2021-22600	Linux	26	High Medium	9.6
Okta	CVE-2023-23529	Google	99	Medium	8.3
Okta	CVE-2021-22600	Apple	72	Medium	8.8

Always expanding integrations

We're building out our Adapter Network every day. With thousands of services and actions available, there are no gaps in your asset data, meaning no blind spots in your attack surface.

Only the cleanest data

It's a herculean effort to get complete and accurate asset data – we know. Our advanced aggregation pipeline constantly normalizes, deduplicates, and enriches your asset data to the fullest.

Full lifecycle automation

Vulnerabilities surface, configurations drift, and policies fail. With bi-directional integrations across your critical systems, your assets are continuously verified for state, cost, and posture.

Shared platform. Shared language.

Security, IT, and Risk teams have different needs for asset data. Axonius customers leverage the platform to unify assessment, operations, and reporting, breaking down organizational barriers every day.

To get started with **Axonius Cyber Assets**, contact us to schedule a demo with our team.

Schedule a demo