Axonius

PRODUCT OVERVIEW

Axonius Exposures

The unified engine for cross-domain exposure management

Exposure data is fragmented by design. Vulnerabilities live in scanners. Misconfigurations live in CSPM tools. Identity gaps live in IAM. Coverage failures live somewhere else entirely. Each tool prioritizes in isolation, producing its own list of "critical" issues, but collectively, they're unactionable without manual correlation.

Axonius Exposures unifies all security findings with deep asset and business context, so teams can see what's truly exposed, focus remediation on what reduces risk, and mobilize fixes across systems and teams at scale.

With Axonius, you gain:

Unified Security Findings

Aggregate and deduplicate findings from hundreds of security tools into a single view. One issue, one record, full asset context.

Triple-Context Prioritization

Combine technical severity with asset criticality and business impact to surface the exposures that actually matter.

Automated Owner Identification

Map every finding to the person or team responsible for the fix — no detective work, no finger-pointing.

Automated Control Validation

Cross-reference findings with active security controls to instantly answer: is this host actually protected?

Remediation Orchestration & SLA Tracking

Trigger direct fixes or route tracked tickets to the systems teams already use with centralized ownership and SLA visibility.

Durable Context

Every finding tied to real assets with security, business, and ownership context that holds as the environment changes.

Prioritized for Action

Customizable scoring that turns overwhelming finding volumes into a focused queue aligned to real organizational impact.

Continuously Covered

Every fix tracked against SLAs and validated — so exposure management stays continuous, not periodic.

> A vulnerability, when viewed solely in isolation using the traditional treatment method based on critical, high, medium and low ratings, is problematic for several reasons.

GARTNER: How To Implement a Risk-Based Vulnerability Management Methodology

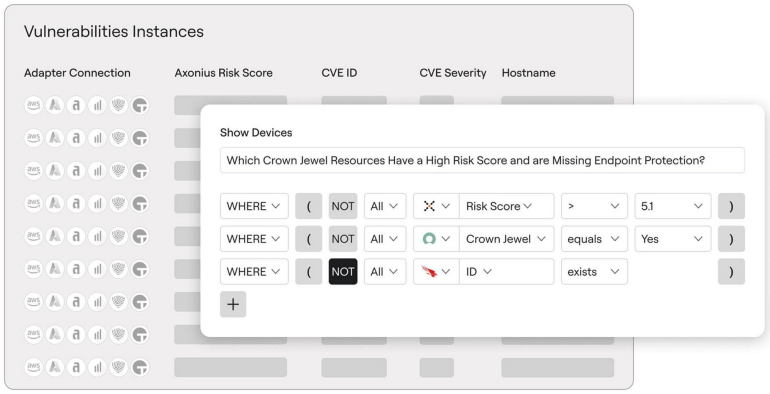
Axonius

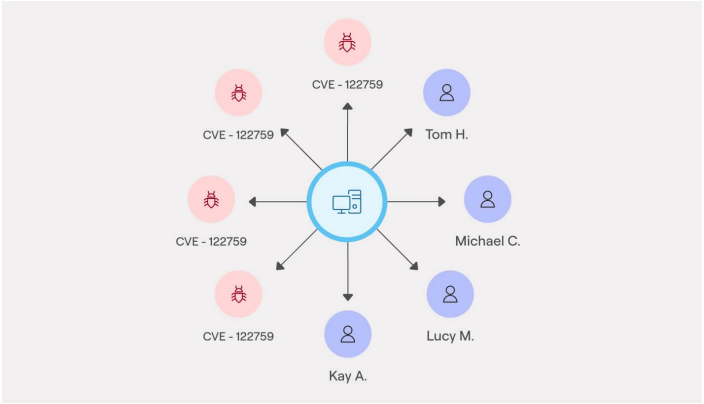
UNIFIED EXPOSURE MANAGEMENT

Every finding correlated, deduplicated, and tied to assets

Scanners, CNAPP, identity tools, and AppSec platforms each produce their own findings, severity ratings, and version of "critical." Teams end up console-hopping or exporting to spreadsheets just to assemble a basic picture.

Axonius ingests findings from 150+ sources, deduplicates them, and ties every issue to the assets it affects – CVEs, misconfigurations, coverage gaps, identity risks. One catalog, no duplicates, full context.





TRIPLE-CONTEXT ENRICHMENT

Security findings meet asset reality and business impact

A critical CVE on a test server and a critical CVE on a production database serving revenue operations are not the same problem — but to a scanner, they look identical. Axonius layers asset context and business context onto every finding.

This is what turns overwhelming volumes into a prioritized queue teams can actually work with — focused on exposures that carry real organizational impact, not just the highest technical severity.

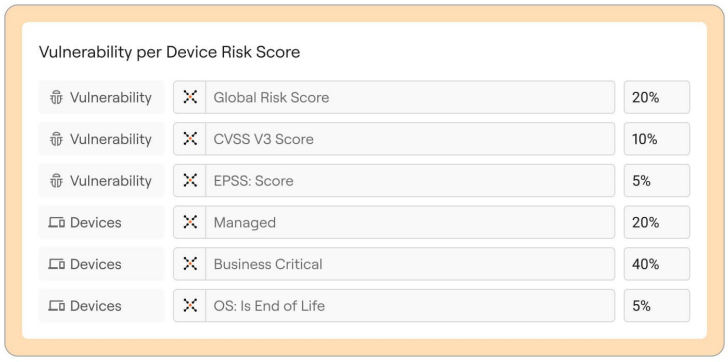
Axonius

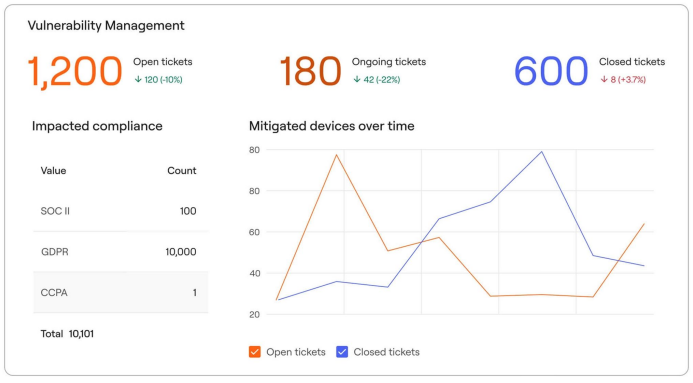
CONTEXTUAL PRIORITIZATION

Risk scoring tuned to your environment

Generic severity ratings treat every environment the same. Axonius lets teams weight exploitability, business criticality, asset sensitivity, and compensating controls into a transparent, customizable scoring model.

The result is a risk score that reflects your reality, where limited remediation capacity should be focused first.





REMEDIATION ORCHESTRATION

Close the loop on remediation - continuously

Identifying exposures is half the problem. Mobilizing the fix is where programs stall. Axonius triggers automated fixes where outage risk is low, and routes tracked, SLA-bound tickets to the right owners when human judgment is required.

Every action and outcome is tracked in one place, giving program owners the visibility to prove progress and keep remediation moving.

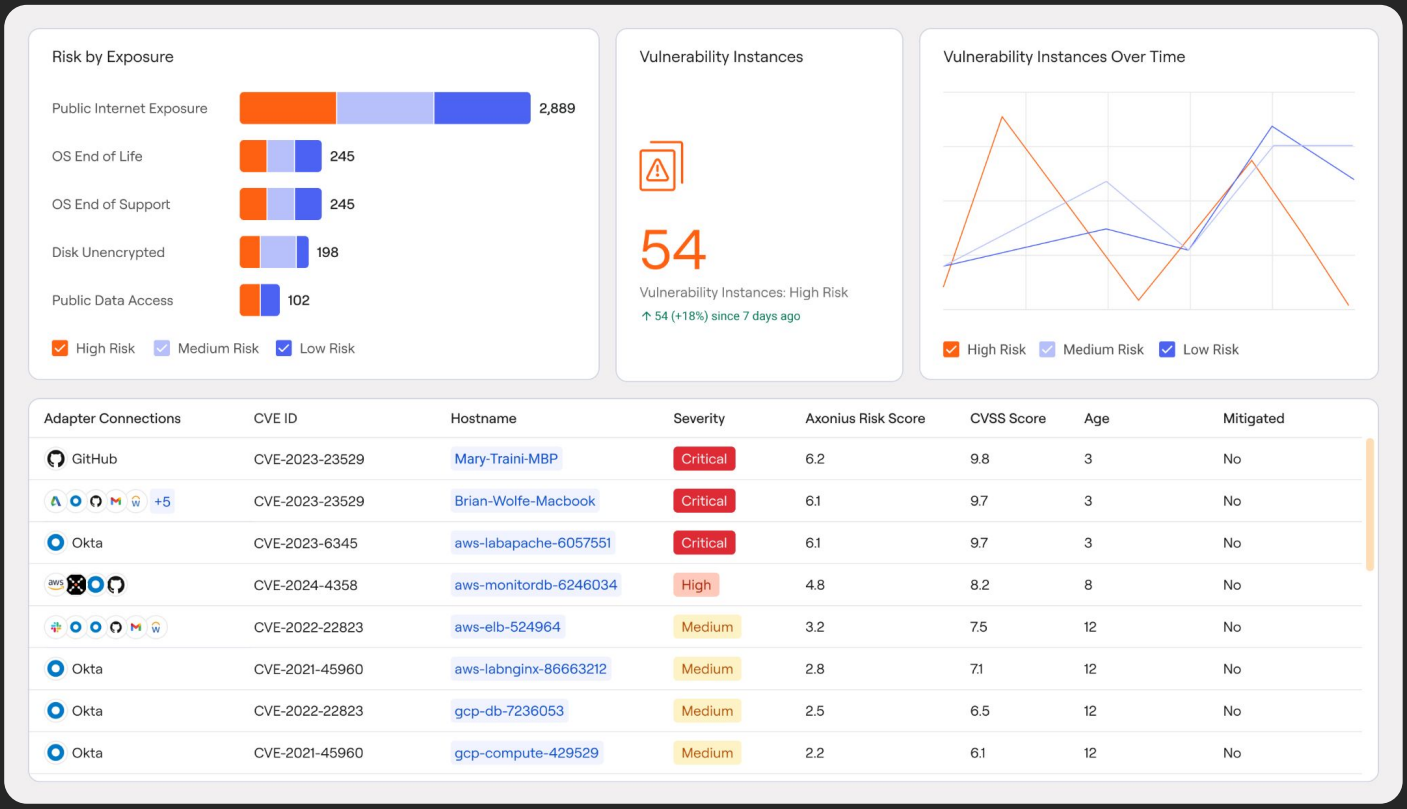
Key Capabilities

Axonius Exposures pairs unified findings with the asset and business context teams need to prioritize, mobilize, and prove progress — all from one place.

Feature	The Axonius approach
Unified Security Findings Catalog	Aggregate vulnerabilities, misconfigurations, and control gaps from all security tools into a single, deduplicated view
Enriched Asset Profiles	View every exposure in full context – linked to asset state, ownership, environment, and control coverage
Structured Query Builder	Build precise, multi-condition queries to investigate exposures based on risk, asset, or business criteria
Flexible Exposure Dashboards	Visualize risk posture, remediation progress, and compliance metrics with customizable charts & graphs
Universal Risk Score	Prioritize exposures using transparent, customizable scoring based on exploitability, business impact, and more
Public Exposures	Identify internet-exposed assets by modeling routes across firewalls, load balancers, and subnets
Real-Time Threat Intelligence	Enhance findings with threat intel signals – like KEV and known exploits – to raise urgency for the most critical risks
Business Unit Ownership	Map exposures to business units or owners to streamline accountability, escalation, and remediation handoff
Asset Graph	Explore how exposures relate across users, devices, applications, and infrastructure to uncover the blast radius
Automated Enforcement Actions	Trigger real-time actions like isolation, policy updates, or access removal to contain and reduce risk
Exposure Remediation Workflows	Design and run remediation flows across tools and teams to track status, assign ownership, and verify resolution
Bi-Directional Ticket Binding	Keep tickets in sync with real-time exposure data – automatically updating status, assignees, and notes

Axonius

Take *action* with Axonius Exposures



Adapter Connections	CVE ID	Hostname	Severity	Axonius Risk Score	CVSS Score	Age	Mitigated
GitHub	CVE-2023-23529	Mary-Traini-MBP	Critical	6.2	9.8	3	No
+5	CVE-2023-23529	Brian-Wolfe-Macbook	Critical	6.1	9.7	3	No
Okta	CVE-2023-6345	aws-labapache-6057551	Critical	6.1	9.7	3	No
	CVE-2024-4358	aws-monitordb-6246034	High	4.8	8.2	8	No
	CVE-2022-22823	aws-elb-524964	Medium	3.2	7.5	12	No
Okta	CVE-2021-45960	aws-labnginx-86663212	Medium	2.8	7.1	12	No
Okta	CVE-2022-22823	gcp-db-7236053	Medium	2.5	6.5	12	No
Okta	CVE-2021-45960	gcp-compute-429529	Medium	2.2	6.1	12	No

Adapter Network

150+ security tool connections — scanners, CNAPP, identity providers, AppSec platforms — ingesting every finding type across the full environment.

Asset Fabric

Every finding correlated to real assets with ownership, business criticality, control state, and dependency context, so prioritization reflects reality, not just severity.

Insights

Exposure dashboards, risk trending, and remediation progress, giving program owners and executives a shared view of posture and progress.

Actions

Automated fixes, tracked tickets, SLA enforcement, and owner accountability, orchestrated across the systems your teams already use.

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

Schedule a demo