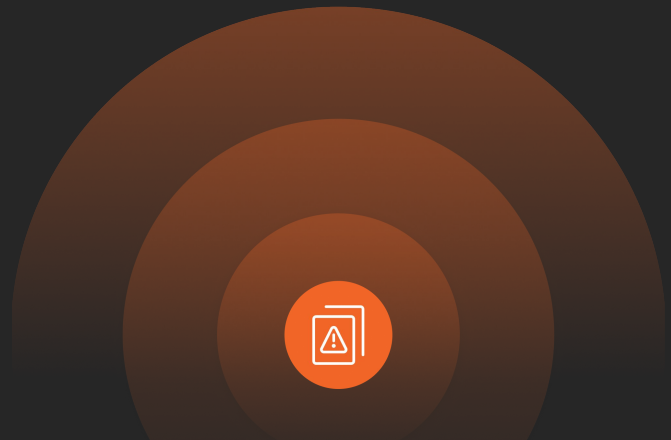


## PRODUCT OVERVIEW

# Axonius Exposures

Take action against exposures  
before they become exploits



Security teams are overwhelmed by more than just vulnerabilities. Misconfigurations, coverage gaps, weak controls, excessive permissions, and more all contribute to the expanding exposure landscape – impacting not just security risk, but also performance, compliance, and cost. Yet these issues are often scattered across disconnected tools and teams, making it hard to see the full picture, let alone take coordinated action.

Axonius Exposures changes that. By unifying all security findings – vulnerabilities and beyond – with deep asset and business context, Exposures helps teams identify what's truly urgent, act with precision, and track progress across their entire environment.

Axonius empowers intelligent action:

- **Unified Security Findings Catalog**  
Aggregate exposures of all kinds from every security tool into a single, normalized view.
- **Contextual Risk Assessment**  
Enrich every finding with real-time asset, security, and business context to uncover what's truly at risk.
- **Custom Risk Scoring Engine**  
Prioritize based on exploitability, asset importance, exposure level, compensating controls, and more.
- **Orchestrated Remediation**  
Mobilize teams and tools with unified workflows, automation, and case management to resolve issues faster.
- **Program-Level Reporting**  
Track remediation progress, validate outcomes, and report on posture improvements across the entire program.

**Achieve Unified Exposure Visibility**

See all exposures in one place, tied to real asset and business context. Axonius gives you a comprehensive view of what needs attention across the entire environment.

**Risk-Based Prioritization That Works**

Axonius correlates exploitability, asset criticality, exposure level, and compensating controls to help teams cut through the noise and focus on the issues that actually matter.

**Streamline End-to-End Remediation**

From triggering fixes to tracking outcomes, Axonius delivers a unified workflow for coordinating remediation across teams and tools – automating where possible.



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.

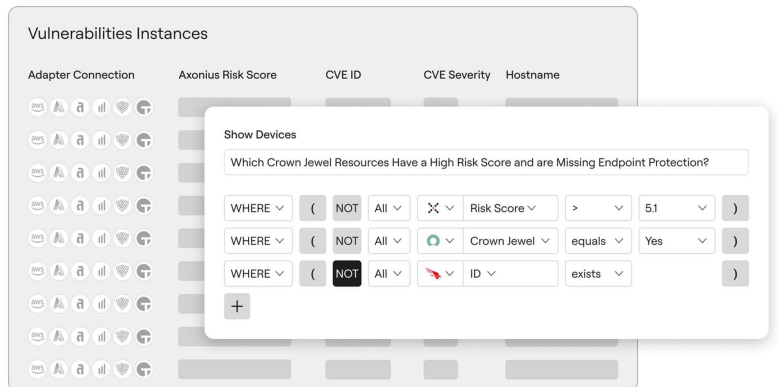
GARTNER: How To Implement a Risk-Based Vulnerability Management Methodology

## UNIFIED EXPOSURE MANAGEMENT

### Turn fragmented findings into actionable insights

Axonius brings together vulnerabilities, misconfigurations, and policy violations into a single, normalized view – so you can finally see your entire exposure landscape without jumping between tools or exporting findings.

By ingesting and correlating data from scanners, config tools, cloud platforms, and more, Axonius eliminates silos and duplicates to deliver one source of truth. Every issue – whether a CVE, a coverage gap, or excessive permissions – is tied to real assets with real business context.

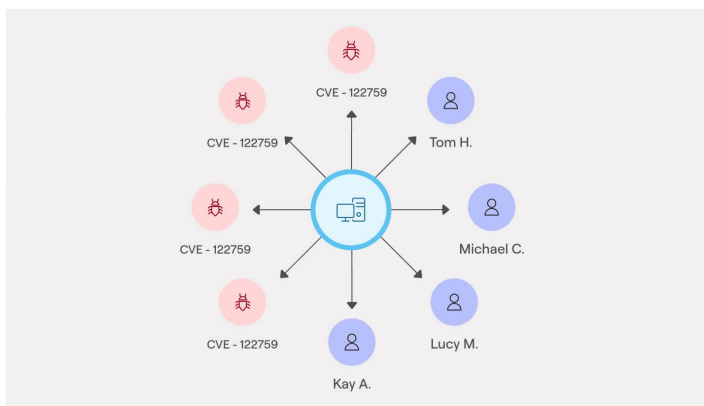


## ENRICHED ASSET CONTEXT

### See exposures with full context to act smarter and faster

Exposures don't exist in isolation – and Axonius makes sure you never treat them like they do. By tying every finding to rich, real-time asset context, teams can understand not just what's vulnerable, but how that risk fits into the bigger picture.

Axonius maps the relationships between software, devices, users, identities, and infrastructure to expose how vulnerabilities propagate across environments. This relational context powers smarter prioritization and enables teams to respond with surgical precision, not broad strokes.

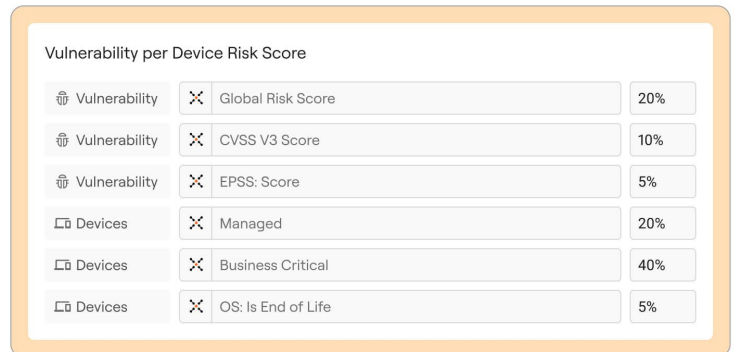


## DYNAMIC RISK SCORING

### Right-size prioritization fit to your capacity

When everything is urgent, nothing gets fixed. Axonius cuts through the noise with transparent, customizable risk scoring that reflects the realities of your environment – not just the severity of a CVE.

Each score is calculated from multiple dimensions: exploitability, business criticality, exposure level, asset sensitivity, and the presence (or absence) of compensating controls. The result is a universal score that reflects true risk – and helps teams align response with the impact that matters.

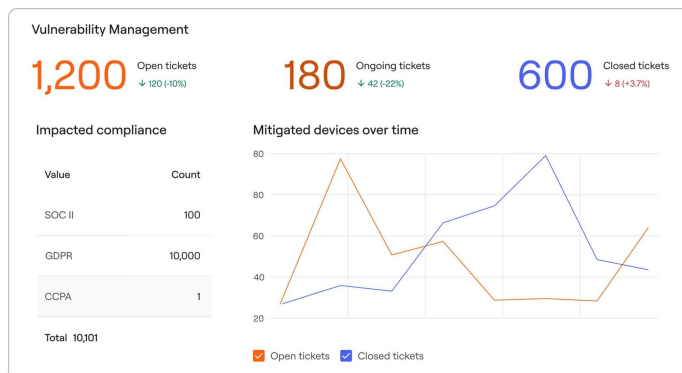


## END-TO-END LIFECYCLE ACTIONS

### Close the loop on remediation efforts - continuously

Remediation doesn't stop at opening a ticket. Axonius delivers a unified, cross-functional workflow to manage remediation from discovery through resolution – across teams, systems, and timelines.

With deep integrations into IT, SecOps, infrastructure, and ticketing tools, Axonius orchestrates assignments, automates actions, tracks status, and audits every step along the way. It's remediation at scale – built for accountability, speed, and clarity.

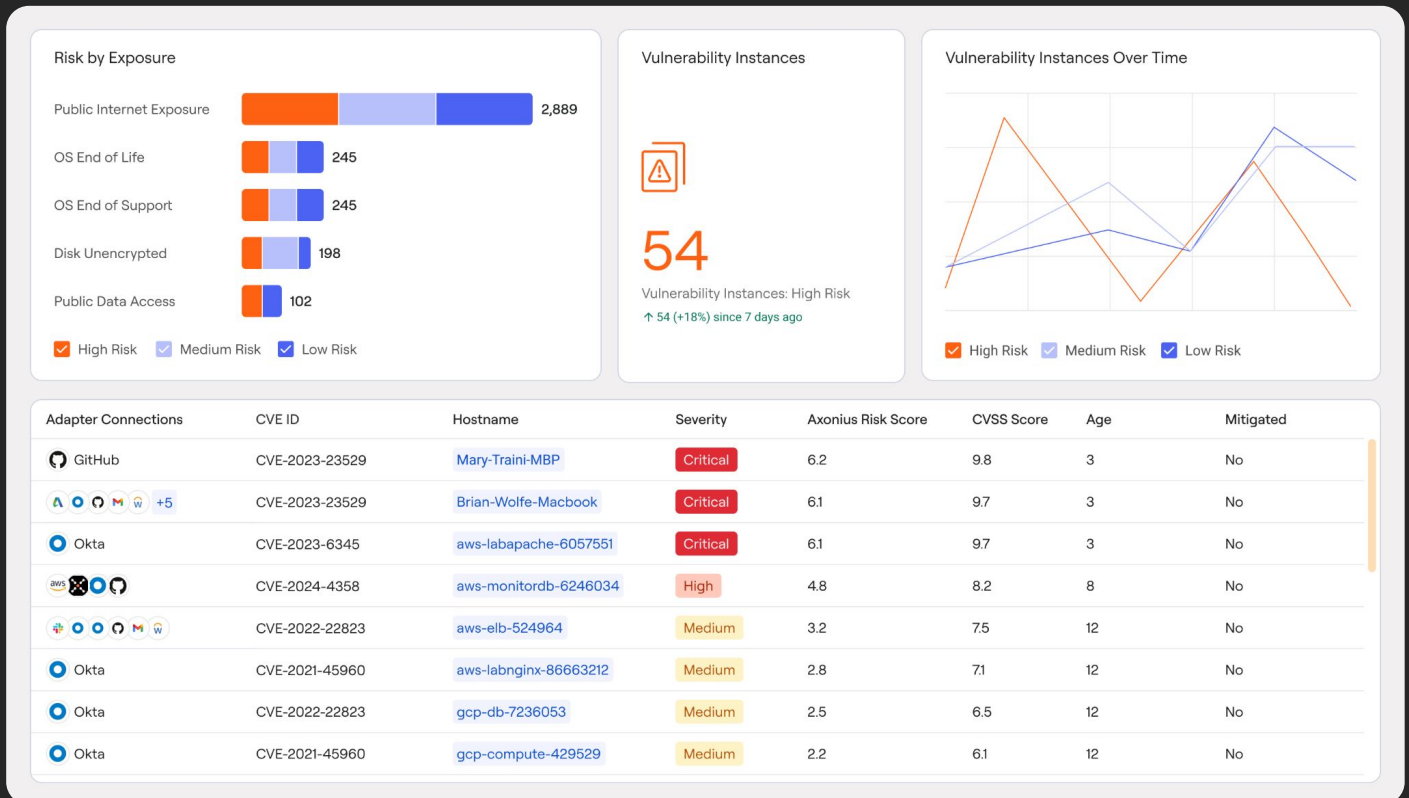


# Key Capabilities

Axonius brings **actionability** to Security and Risk teams by unifying exposure data with real asset and business context to drive smarter prioritization, faster remediation, and measurable risk reduction.

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

# Take *action* with Axonius Exposures



## Comprehensive risk clarity

Forget silos and partial visibility. Axonius unifies vulnerabilities, exposures, and misconfigurations into one platform, providing a holistic and actionable view of your total risk landscape.

## More proactive actionability

Axonius uncovers exploitable paths and at-risk assets, empowering teams to take preemptive action and shrink the attack surface before adversaries strike.

## Risk context that matters

You won't get stuck with missing intel. Axonius enriches every risk with business context, mapping relationships between assets, identities, and infrastructure to help you act smarter.

## Designed for cross-functional teams

No more juggling tools and teams. Axonius centralizes planning, tracking, and auditing to streamline the entire remediation lifecycle and ensure accountability.

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

[Schedule a demo](#)