AXONIUS

Minimize Your Attack Surface with Axonius

How accurate is my asset inventory?

The question is simple, but often, the answer is elusive.

Having 360 visibility into your digital assets with full context is table stakes for all businesses. It's not just about knowing ***what*** assets you have, it's about knowing ***how*** those assets interact with each other, and ***when*** to take remediation action. Any asset missing a security control, is misconfigured, or has a vulnerability increases the risk associated with your total attack surface.

A comprehensive solution provides the foundation to identify and minimize all attack vectors - mitigating the impact of threat exposure.

Security teams today are struggling with:

- **More dynamic assets**
  → difficulty in maintaining an accurate attack surface assessment
- **Domain-specific silos**
  → inability to see all coverage gaps/exploit paths
- **Shadow IT**
  → invalidating insights from traditional tools

Unify attack surface investigation

The right solution gives you a source of truth for all your assets

Reduce time to remediation

The right solution integrates with your tech stack to automate remediation

Correlate asset intelligence

The right solution provides contextualized insights across your asset relationships

> By 2026, organizations prioritizing their security investments based on a coântinuous exposure management program will be ***3x less likely*** to experience a breach.
>
> GARTNER, IMPLEMENT A CONTINUOUS THREAT EXPOSURE MANAGEMENT PROGRAM, JULY 2022

Managing your attack surface is not *just* a security problem. It impacts your business, too.

The consequences of threat exposure remain greater than ever.

Regulatory pressure

Financial, legal, business and operational impact

Competitive forces

Security and privacy have become key pillars of customer trust

Reputational damage

PII/PHI/PCI/IP data breaches are hard to recover from

A thorough exposure management strategy plays a critical role in aligning Security and IT with the business. That said, why are companies struggling with the right approach to attack surface management?

Today's approaches to attack surface management fall short

Common approaches miss the mark because they were built to support a finite number of static, and already managed assets.

Today's approach	Why it doesn't work
Spreadsheets and/or relying solely on CMDB	Manual and error prone; CMDBs do not provide security posture insights
Domain-specific tools for vulnerability scanning	Lose the full picture view, leading to uninformed decision making
Custom queries and dashboards from event data	Disparate events do not uncover threat exposure in a contextualized/prioritized way

When you have good cybersecurity situational awareness, you can make an informed decision and make your cyber defense strategy more effective and efficient. The information that we get from Axonius is one of the elements that support this process.

TIM LEE, CISO, CITY OF LOS ANGELES

Axonius gives security teams unmatched awareness into their full attack surface

With Axonius, Security and IT have a trusted source for information around the potential blast radius and impact of an incident, and a reference to narrow the scope of what to investigate and what to fix.

Manage and optimize assets

Prioritize and remediate security vulnerabilities

Contextualize & accelerate incident response

Role	Responsibility	Why Axonius
Security leadership/executives (CISO/CSO; VP of Security; Head of Engineering)	Protecting against breach; keeping security teams funded and performing; compliance outcomes	**The source of truth for all critical systems.** Axonius surfaces risk across your digital assets, while also serving your team's need for day-to-day issues
Security managers (Director/Manager of Security/InfoSec; Head of Security Ops; Head of Engineering Platform Services)	Performance and coverage of all related functions; prioritizing efforts and allocating resources; reporting security efficacy up to leadership	**A shared platform service for any technical team.** Axonius is the central operational hub to share data and insights within security and adjacent teams in IT
Security practitioner Security Operations/ SOC Manager; Security/SOC Analyst; Security Engineer	Timely closeout of incidents; continuous threat hunting; documenting incident response procedures	**The go-to platform in any security event.** Axonius is the trusted source of information to understand potential blast radius of an incident to narrow scope and investigate a fix.

Want to learn more about how Axonius can help to minimize your attack surface?

Learn more

AXONIUS