Axonius

3 projects to kickstart your cyber asset attack surface management strategy

Tips for minimizing your attack surface exposure with Axonius

All organizations inevitably experience digital asset sprawl that expands the attack surface. Domain-specific security tools for endpoints, identities, cloud infrastructure and more are siloed and miss the bigger picture, leaving blind spots that lead to overlooked exposure.

Axonius unifies attack surface investigation and remediation with a comprehensive asset intelligence platform purpose-built to close exploit paths across your digital footprint. Let's breakdown the strategies that can help to drive your attack surface management strategy.

Axonius brings your attack surface management strategy to the present

As your asset landscape changes, so must your asset attack surface management strategy. Here's how Axonius helps.

Traditional asset mgmt approaches	with Axonius
Manual efforts to aggregate asset data across spreadsheets	Correlate asset data in minutes with our API-first approach to integrations
Unknown and/or rogue assets remain unidentified	One platform to identify assets and security gaps for both managed and unmanaged assets
Difficulty in identifying and prioritizing vulnerabilities for remediation	Automatic identification and orchestrated remediation of critical vulnerabilities across endpoints

Our customers take on average

14 days
to go production

57%
Assets secured growth (in 6 months)

90%
Remediation automation growth (in 6 months)

Getting started with your Axonius deployment

Security teams in companies of all sizes and across industries trust Axonius as the go-to platform to minimize their attack surface.

3 quickstart projects to *minimize your attack surface*

- Manage and optimize assets
- Remediate security vulnerabilities
- Accelerate incident response

1. Manage and optimize assets

The most foundational way to minimize your attack surface is to have complete and accurate awareness of all assets across all critical systems.

By 2028, investments in proactive technologies that improve visibility and reduce exposure will grow twice as fast as investments in reactive technologies that detect and respond to incidents.

Gartner, Innovation Insight: Attack Surface Management (2024)

Use cases with Axonius

Close High-Risk Coverage Gaps

Missing endpoint agents, missing vulnerability scans, rogue devices, exposed credentials, CMDB reconciliation, migration planning, overprovisioned SaaS

Verify Proper Asset Usage and Ownership

Shadow IT sprawl, Unsanctioned/EOL software and SaaS, Unmanaged/EOL hardware, tagging assets, offboarding employees

Maximize ROI on Security Spend

Unused software licenses, over budgeted SaaS, extreme logging & observability cost

Measuring ROI

Increased percentage of compliant asset coverage

Gain a faster path to compliance by ensuring your digital assets are consistently covered, meet the bar of security posture, and pass regulatory requirements

Reduced time spent collecting and assessing asset data

Streamline your attack surface assessment process with automated data aggregation and correlation, freeing up valuable time to focus on mitigation efforts

Reduced operational and licensing costs

Cut unnecessary expenses without impacting the business by uncovering waste, unused resources, or excessive operations

2. Prioritize & remediate vulnerabilities

"We can now see the security tooling that's deployed and vulnerabilities that potentially exist...this helps increase our security posture, and it's definitely provided a tremendous amount of value to be able to continue to scale our business and program."

Chaim Mazal,
Chief Security Officer
Gigamon®

Use cases with Axonius

Patch Vulnerable Systems
Assess software/hardware/cloud vulnerability impact, prioritize allocation to updates, build runbooks to deploy changes

Resolve Misconfigurations
Fix bad settings ("toxic combinations"), mitigate policy/config drift, remove excessive permissions

Address Weak Controls
Accelerate compliance mapping, optimize SaaS security & usage, perform risk assessments

3 months
for Gigamon to get full visibility into the company's threat landscape across all assets

Measuring ROI

Reduced vulnerability exploit time

Shrink the threat exposure window by rapidly identifying and addressing vulnerabilities before they can be exploited

Increased percentage of patched systems

Enhance your overall security posture by keeping your systems up-to-date

Reduced downtime and business disruption

Prevent costly scenarios by swiftly remediating vulnerabilities that impact critical systems

3. Accelerate incident response

"We have a better understanding of 'what's out there' than ever before, and can take proactive steps to mitigate any issues, vulnerabilities, or problems."

Kyle Levenick,
Program Director For
The It Security & Risk Team

TEXAS A&M UNIVERSITY

Use cases with Axonius

Help Triage

Contextualize alerts & issues, enrich in scope asset data, visualize the blast radius

Perform Investigations

Assess vulnerability reach, threat hunting, historical incident review, forensics analysis

Run Remediations

Automate security workflows, report on resolved issues, investigate unresolved incidents, set enforcement baselines

Measuring ROI

Mean time to inventory

Helps security analysts correlate alerts with data to answer questions like:

- Which devices and users are associated with the alerts?
- What software is/was running on the device?
- Which known vulnerabilities existed on the device?

Dwell time

Speeds up incident response investigations with rich, correlated data. Search for attributes of a particular device or user in order to triage alerts.

Reduce threat RCA time

Helps security operations teams cut down on chasing false positives by quickly assessing threat exposure during triage

Cost of an incident

Makes asset identification quick and simple, reducing the time and cost spend on investigation.

Mean time to respond (MTTR)

Allows SOC team to analyze more alerts in a shorter period of time, thereby increasing visibility and reducing MTTR

Mean time to detect (MTTD)

Provides enhanced visibility into assets (managed and unmanaged) for security operations teams to be more confident in their MTTD metric

"With Axonius, now we can do a quick query, identify which business owns that IP or that asset, and reach out to that business to say, "listen, there is a vulnerability within this asset and we need to remediate it."

Dan Fabbo, Manager Of Security Engineering

cimpress

Want to learn more about minimizing your attack surface with Axonius?

Learn more

Axonius