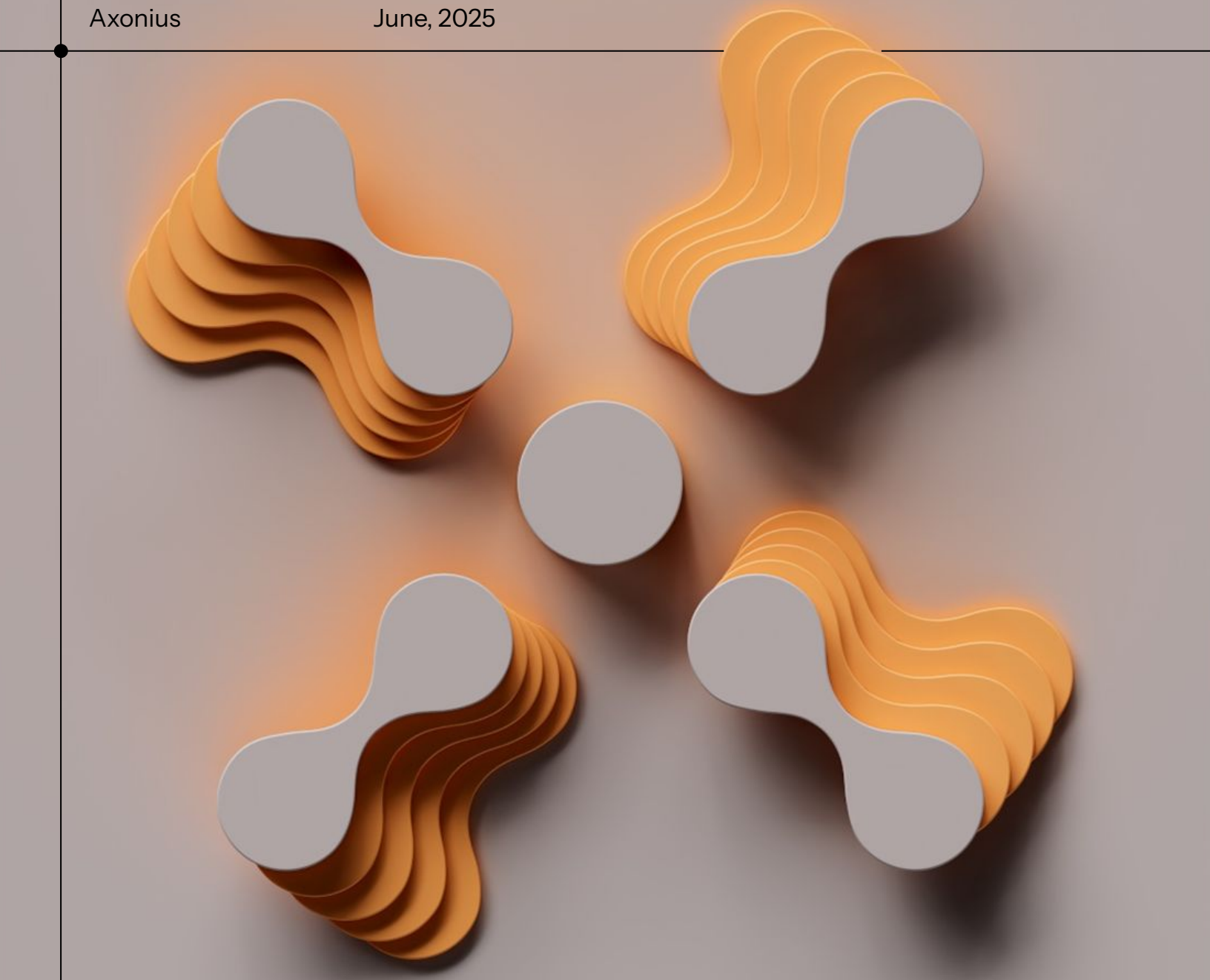
EBOOK

Axonius for *Continuous Threat and Exposure Management (CTEM)*

Axonius June, 2025



Axonius

Table of Contents

Introduction

Continuous Threat Exposure Management (CTEM) has emerged as a strategic approach for organizations to discover and manage cyber risks by providing pragmatic steps for continuously and proactively identifying, prioritizing, and mitigating security risks.

Through the *Axonius Asset Cloud*, we help organizations adopt the CTEM approach across their entire infrastructure regardless of location — remotely located, on-prem, in public clouds, or private clouds.

This technical ebook introduces the CTEM framework and how the Axonius Asset Cloud helps organizations within each step of a CTEM program.

Architectural Principles

This technical ebook is grounded in three core principles:

01

Strong alignment to CTEM

CTEM provides a robust framework with five steps, principles, and best practices. CTEM is based on real life observations of how organizations should approach risks in a proactive and continuous way. By leveraging CTEM as the main driver for this ebook, we ensure strong alignment to your security and risk goals.

02

No silver bullet

CTEM is an organization-wide approach. As such, it requires a holistic strategy — inclusive of processes, multiple technologies, and people — to be successful. Solutions like Axonius, while crucial for CTEM, should not be viewed as a silver bullet for success.

Technologies that position themselves as a silver bullet should also be viewed with caution as they may introduce gaps in your strategy such as breadth of support (coverage across on-prem, public cloud, and multi-cloud planes), processes, and adequate staffing.

03

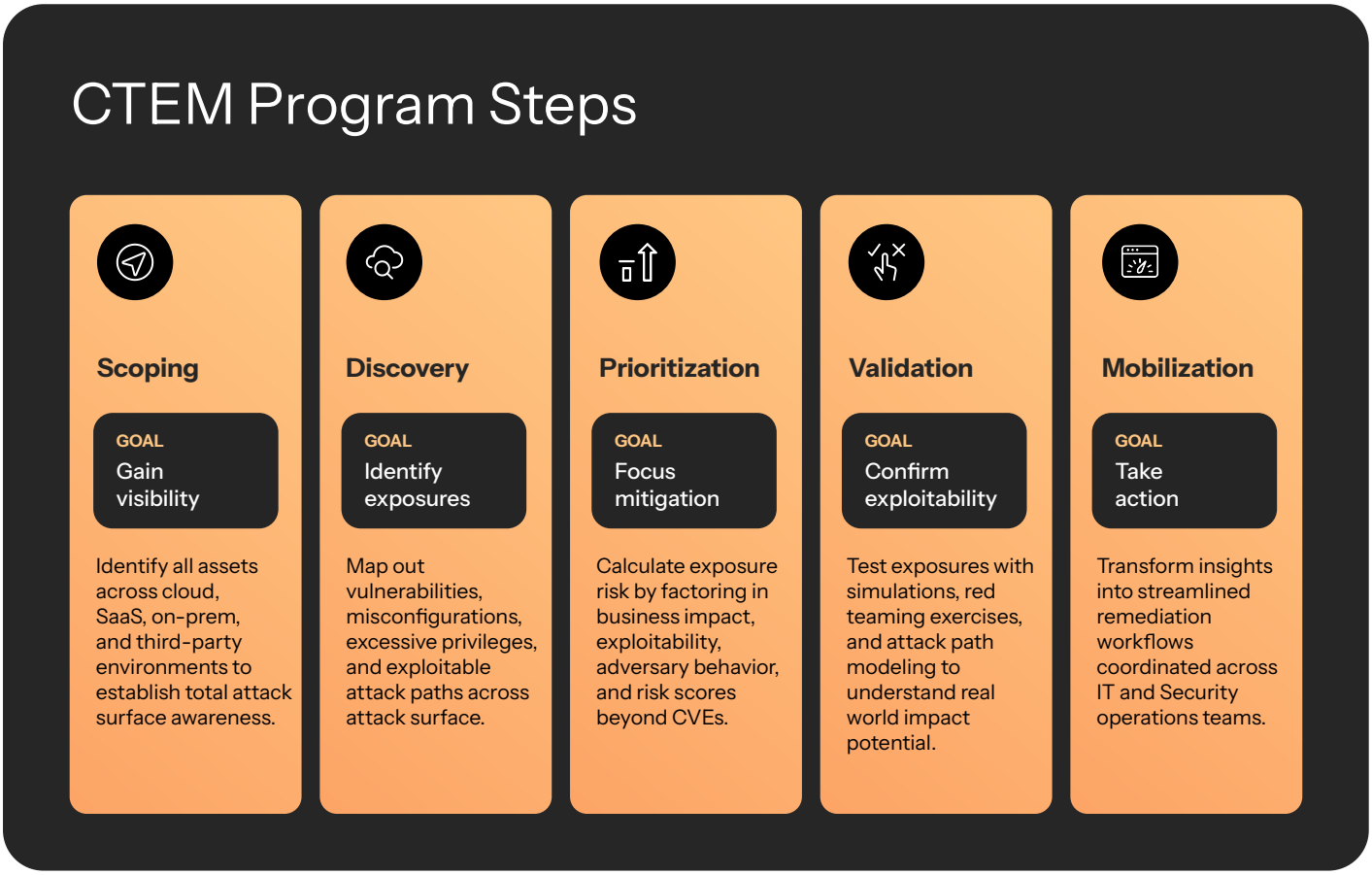
Connection to technology

As companies adopt and invest in CTEM, they need a logical understanding of how technology can be deployed at each step in a beneficial way. Each CTEM step covered in this ebook is accompanied by a section on how Axonius can be applied to this area with screenshots and links to relevant features and public documentation.

What is *CTEM?*

Cybersecurity teams face relentless pressure. As technology sprawls across distributed environments, attack surface widens, risks multiply, and responding effectively becomes increasingly challenging. Continuous Threat Exposure Management (CTEM) is a proactive and ongoing approach that aims to identify, assess, and reduce an organization's exposure to cyber threats. Gartner® coined the term and concept of CTEM in 2021.

CTEM is not a specific technology or tool, but rather a comprehensive framework designed to help organizations improve their security posture in response to the rapidly evolving threat landscape. The framework consists of five core stages:



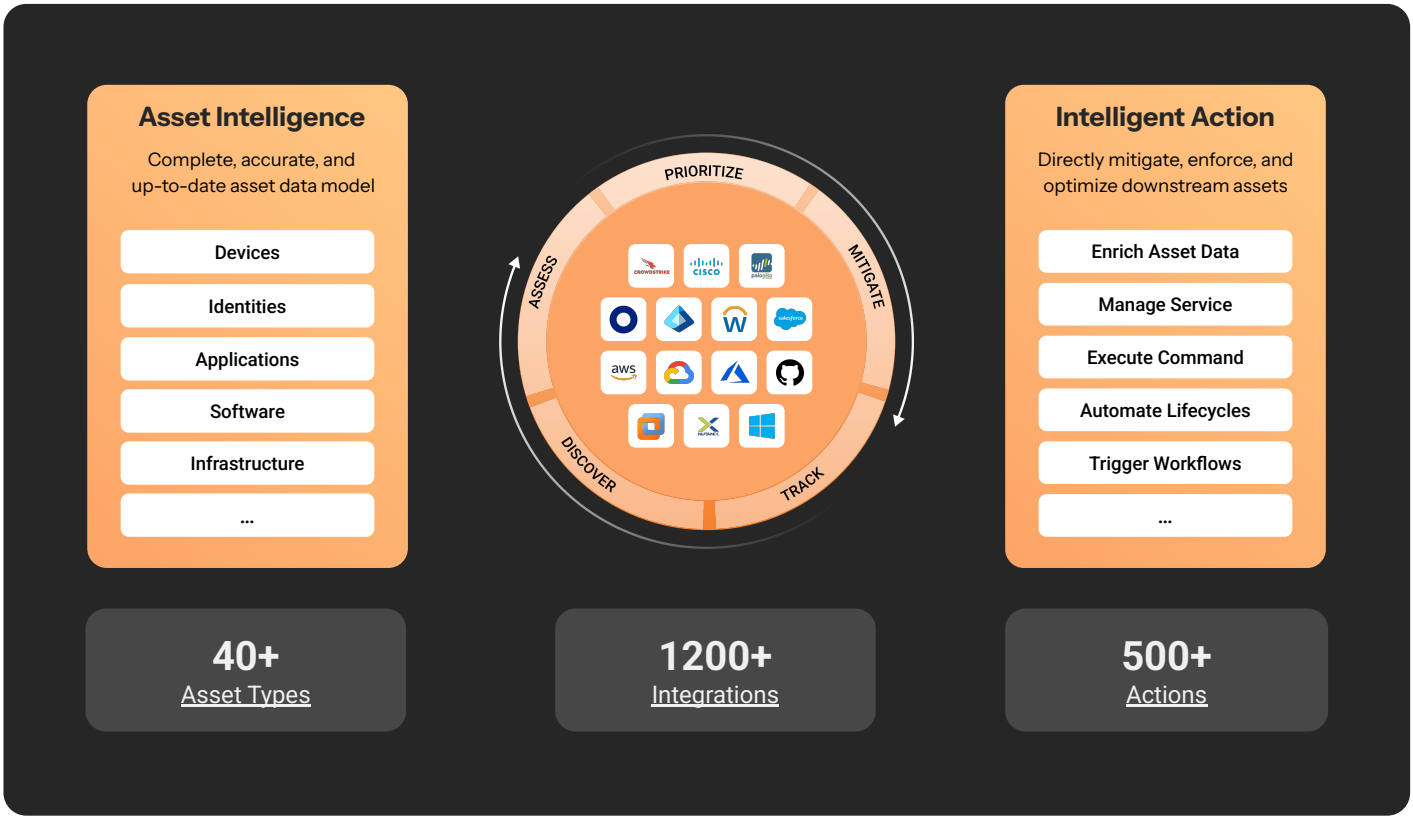
These stages form a continuous cycle that involves regularly scoping organizations assets, identifying and prioritizing risks, validating if risks can be materialized, and implementing mitigation strategies.

By shifting from reactive vulnerability management — i.e. triggered by the introduction of new CVEs and escalated if they make the headlines (aka celebrity CVEs) — to a continuous approach, organizations get multiple benefits: from the ability to identify risks as new assets are introduced to your environment, to prioritization by focusing on risks that could disrupt business operations, to the continuous improvement through repetition and automation.

What is *Axonius?*

Axonius, as a leader in cyber asset management, delivers visibility and actionability across all digital assets. Through the Axonius Asset Cloud, organizations get a global view of all assets interacting with their data and processes alongside their security posture and risk:

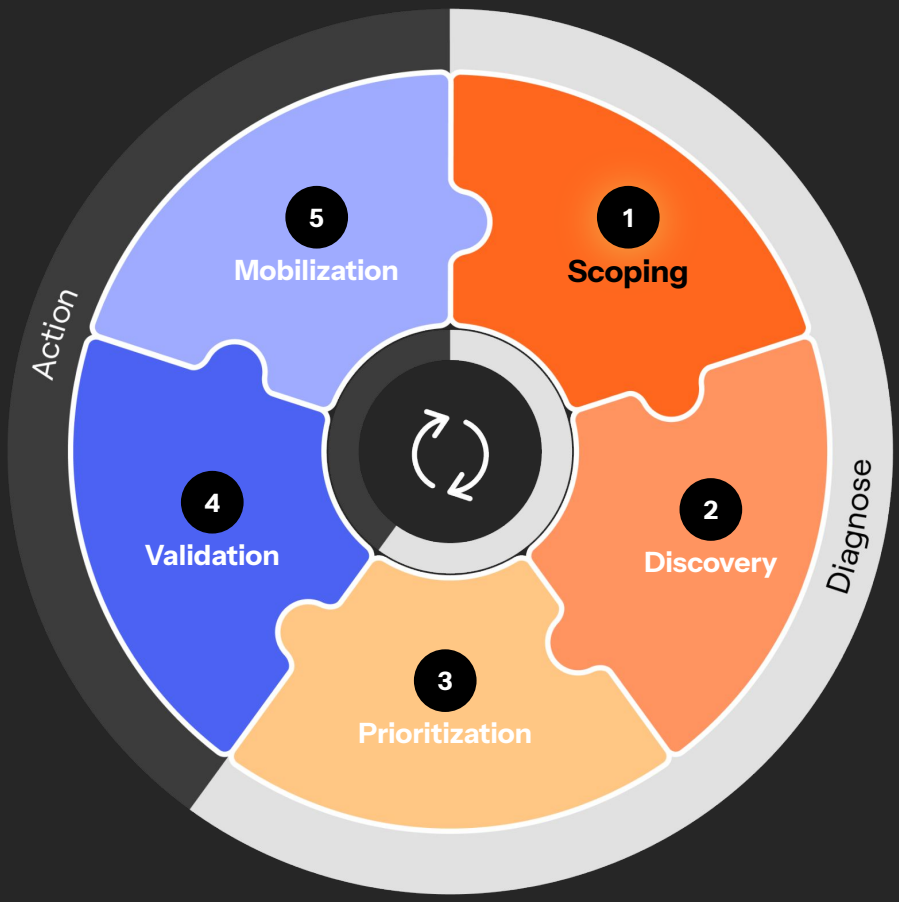
Powered by the largest asset integration network — supporting over 1200+ integrations, 40+ asset types, and 500+ automated actions, Axonius delivers deep asset intelligence while empowering teams to take direct action to reduce risk, improve performance, and control costs.



Axonius has built five products on top of the Axonius Asset Cloud, each designed to address the specific needs of different teams and use cases. By leveraging the same powerful underlying platform, each product benefits from unified asset intelligence, bi-directional integrations, and actionable insights — tailored to different operational challenges:

- **Axonius Cyber Assets**
  Ensure every asset across every system is known, compliant and protected.
- **Axonius Software Assets**
  Gain actionable visibility into software usage across the organization.
- **Axonius SaaS Applications**
  Inventory your SaaS landscape, mitigate risks, and optimize software spend.
- **Axonius Exposures**
  Unify exposure findings, correlate and rank risks, and execute mitigations.
- **Axonius Identities**
  Unify all identity artifacts in one place to transform fragmented data into insights.

By establishing a source of truth for assets, insights, and actionability, Axonius helps organizations adopt the CTEM approach with consistency across their entire infrastructure on-prem, in public clouds, and private clouds.



The 5 steps of *CTEM*
(and how Axonius can help)

Axonius

STEP 1:

Scoping

GOAL

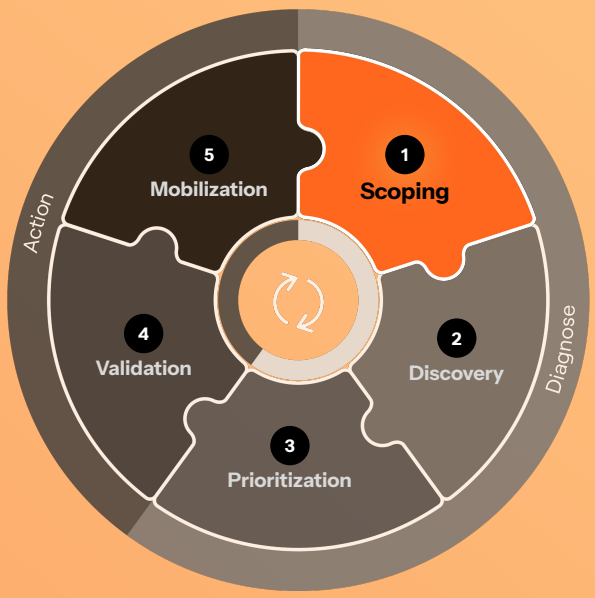
Gain Visibility

Identify all assets across cloud, SaaS, on-prem, and third-party environments to establish total attack surface awareness.

THE CHALLENGE

How do we measure the business value of our assets?

- Dealing with incomplete and inaccurate asset inventory data
- Working with unclear mappings between assets and workloads
- Knowing where to apply value measures in prioritization models



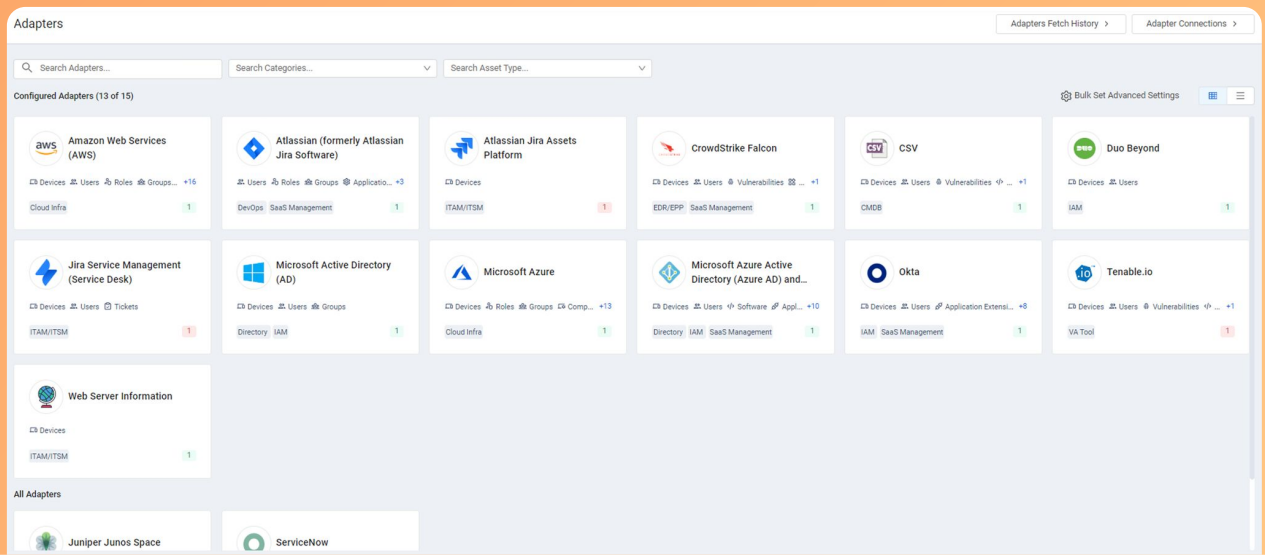
Scoping With Axonius

Axonius supports scoping by identifying all assets interfacing with your data and processes. Axonius achieves scoping through adapters, discovery logic, and continuous discovery.

Adapters

To identify assets, Axonius integrates with your IT, Security, and business solutions using pre-built integrations known as adapters. As of June 2025, Axonius supports over 1,200 native adapters capable of identifying over 40 asset types regardless of where they are hosted.

Adapters Page

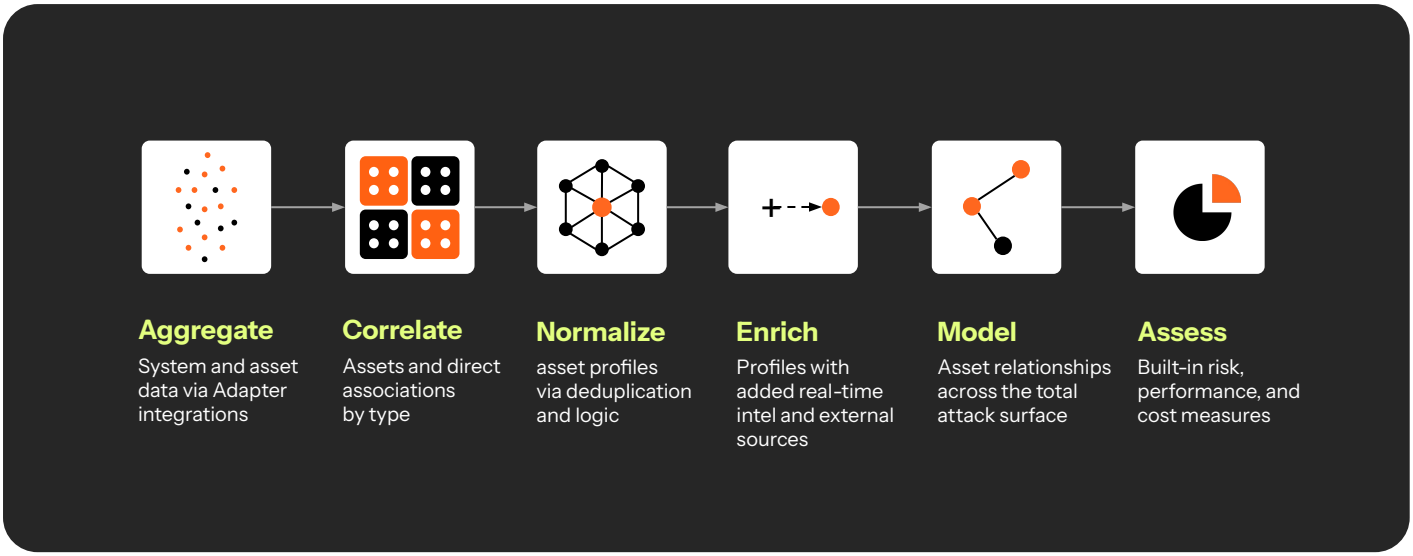


Adapters are integrated using native and open APIs, eliminating the need for agents or network tapping that introduces deployment friction, maintenance burden, and limitations in identifying shadow IT or assets outside your network.

Discovery logic

After collecting asset information, Axonius initiates its mapping phase, (aggregation, correlation, deduplication, normalization and enrichment) to ensure your asset scoping is both complete and accurate, with assets uniquely identified, enriched, and free from inconsistencies. The logic also sets the foundation for future steps in the CTEM process, like discovery.

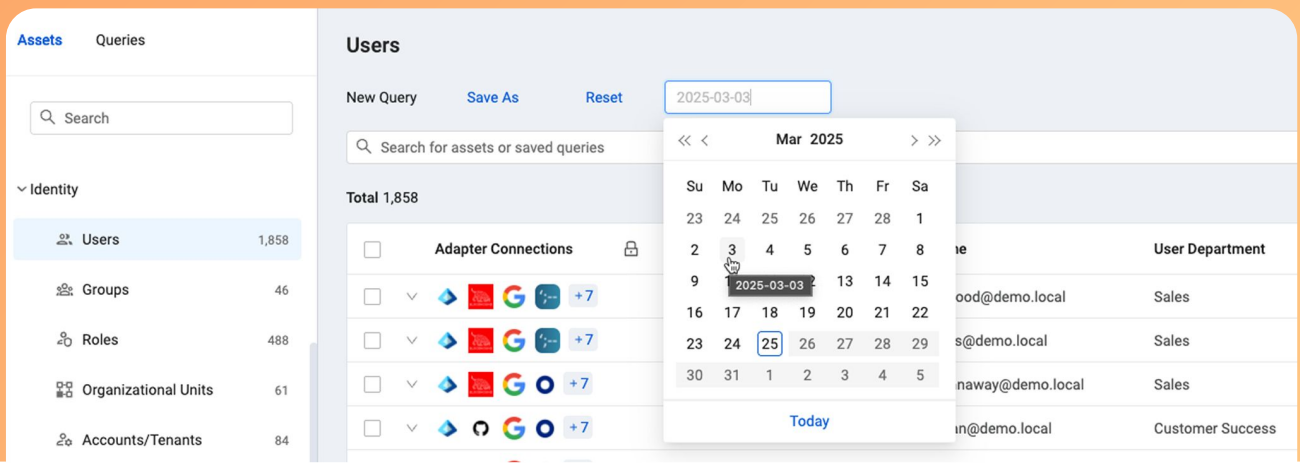
For example:
By identifying a laptop under management accessing your internal applications, but missing your endpoint protection (EPP), you identify a blind spot in coverage.



Continuous Discovery

CTEM is a continuous process. As such, it requires the scoping of assets to be run continuously across your environments. Axonius provides a recurring schedule and real-time adapters to ensure changes in your assets are regularly and automatically captured. Axonius also provides historical snapshots of your attack surface, giving you the ability to track changes in the attack surface over time and uncover gaps like assets missing in action.

Through continuous discovery and snapshots,
you can see the scope at any date



STEP 2:

Discovery

GOAL

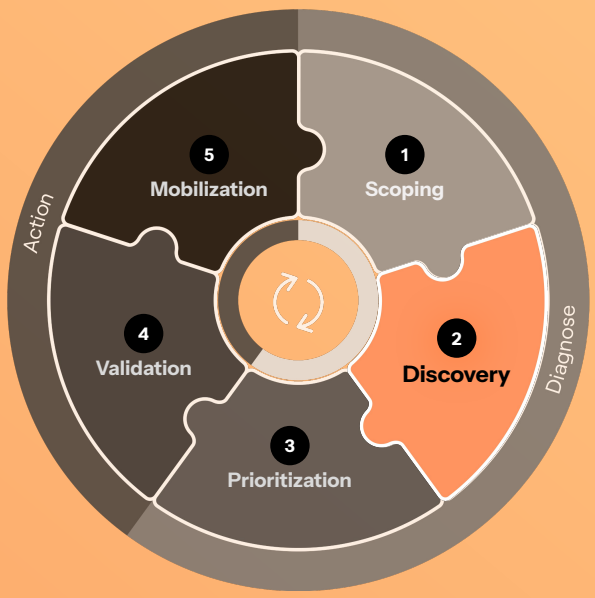
Identify Exposures

Map out vulnerabilities, misconfigurations, excessive privileges, and exploitable attack paths across attack surface.

THE CHALLENGE

How to assess all exposures in one place?

- Disjointed tools generate a lot of noise - duplicates, false positives, etc.
- Understanding which exposures are exploitable and how, and their risk
- Often missing relevant context, relationships, and real-time threat intel



Discovery with Axonius

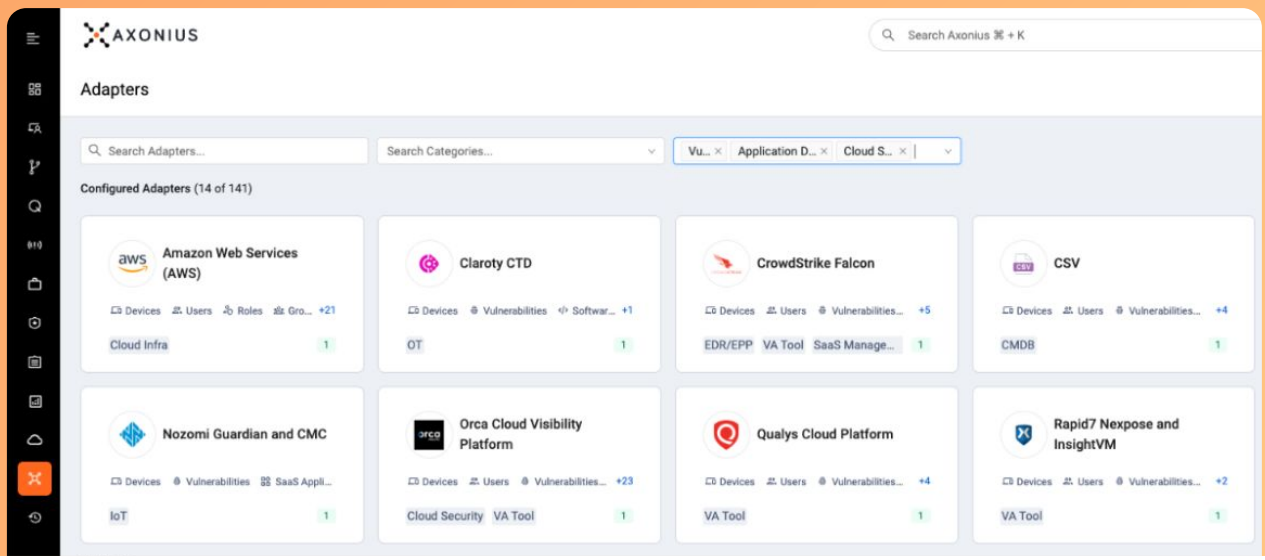
Axonius supports discovery by providing a single source of truth for exposures. The source of truth contains exposures reported by all your security tools alongside exposures identified by Axonius.

Axonius achieves discovery through exposure and vulnerability adapters, discovery logic, static analysis and enrichments, exposures, misconfigurations (through queries and dashboards), and external to internal mapping.

Exposure and vulnerability adapters

In addition to scoping assets, Axonius adapters are also used to gather rich security context discovered by your existing IT and security solutions. As of Mar-25, over 140 adapters (from our adapters documentation, search for “vulnerabilities” or “exposures”) provide information about vulnerabilities, cloud security, and application development exposures. These exposures range from traditional vulnerability scanners, to endpoint protection platforms, to threat intelligence feeds, to breach and attack simulation (BAS), to SAST and DAST scanners, CNAPP platforms, and much more.

Adapters reporting exposures



Discovery logic

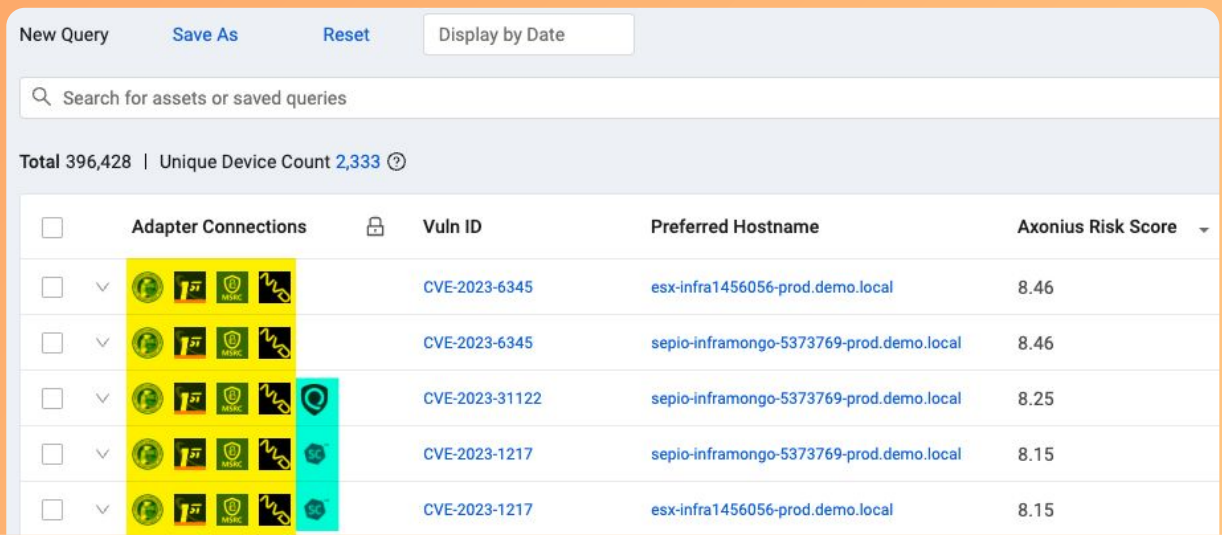
Axonius leverages the same discovery logic from scoping assets to aggregate, correlate, and deduplicate your exposures. That gives your teams an accurate list of exposures that are uniquely identified, enriched, and free from inconsistencies.

Vulnerability Enrichments

As part of the discovery logic, Axonius enriches all your assets (from the scoping step) and exposures (in the discovery step) with data from major vulnerability context providers such as NIST National Vulnerability Database (NVD), CISA Known Exploited Vulnerabilities (KEV), Exploit Prediction Scoring System (EPSS), and the Microsoft Security Response Center (MSRC) along with any of your desired threat intel feeds:

Vulnerability Instances

Vulnerability instances (a type of exposure identified by Axonius) with information reported by your adapters (in green) and by Axonius enrichments (in yellow). The first two vulnerability instances are found exclusively through enrichment and note reported by adapters (either through a missing scan or the lack of vulnerability scanner in the asset)

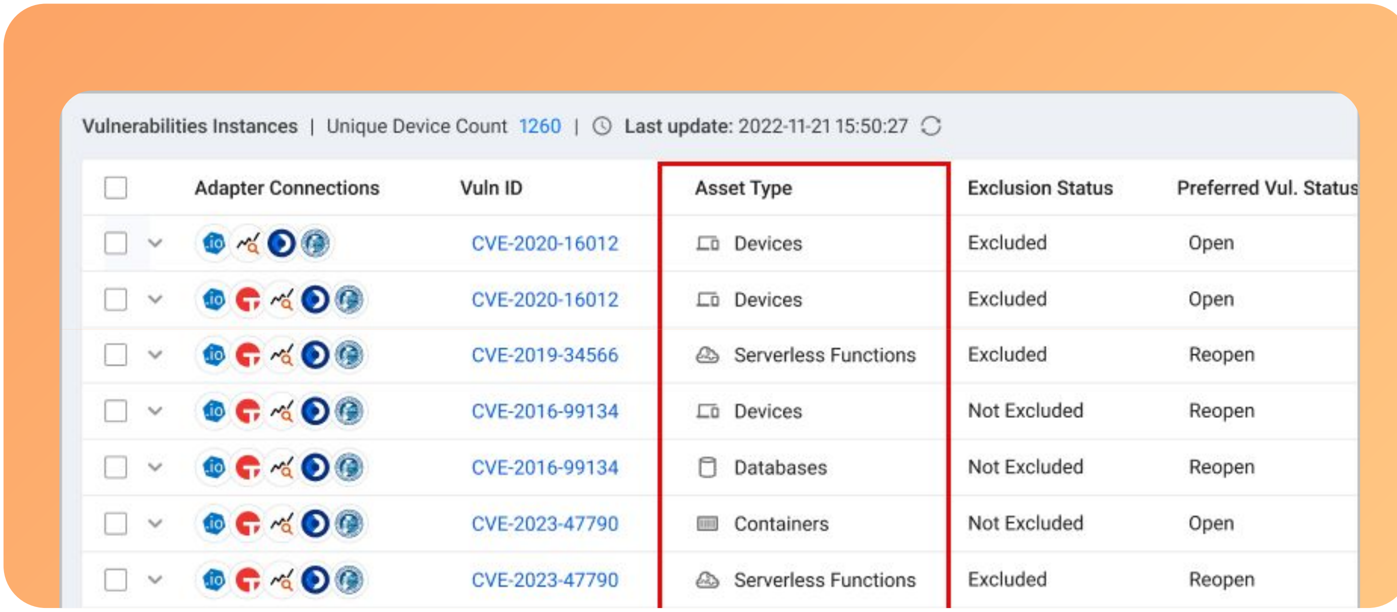


This information is used in three ways: to enrich vulnerabilities already found by your security solutions, to identify emerging vulnerabilities faster than the scanner cadence, and to identify vulnerabilities in assets without a scanner or a recent scan.

	1 Vulnerabilities found by your systems	2 Vulnerabilities *not yet* found by your systems	3 Vulnerabilities where scanners are not present
140 + Adapters	- Aggregated scanned data	- Scan failures - Waiting for re-scan	- No scanner present
Enrichments	- Complementary context	- Initial context	- Vulnerability Context
Outcomes	- Better vulnerability intelligence	- Reduce time to recognition - Reduce pressure on scan SLAs - Mitigate scan failures	- Discover exposures in assets without scanners

Exposures

Axonius aggregate exposures — from all your assets across, on-prem and cloud infrastructure — under the exposures category.



Vulnerabilities Instances | Unique Device Count 1260 | Last update: 2022-11-21 15:50:27

Adapter Connections	Vuln ID	Asset Type	Exclusion Status	Preferred Vul. Status
	CVE-2020-16012	Devices	Excluded	Open
	CVE-2020-16012	Devices	Excluded	Open
	CVE-2019-34566	Serverless Functions	Excluded	Reopen
	CVE-2016-99134	Devices	Not Excluded	Reopen
	CVE-2016-99134	Databases	Not Excluded	Reopen
	CVE-2023-47790	Containers	Not Excluded	Open
	CVE-2023-47790	Serverless Functions	Excluded	Reopen

Each exposure item combines the security context (i.e. vulnerability CVE, technical score, threat intelligence feed data) with asset context, and business context. This information is used in subsequent CTEM steps to help prioritizing and mobilizing the right teams.


Unified Context
Get a full picture of the risk across security, asset, and business context.
Security Findings
Asset Intelligence
Security Context
Vulnerability Scanner
Endpoint Protection/AV
Threat Intelligence
...
Asset Context
Asset online
EPP coverage
Asset state
Internet traffic
Linked to admin
Domain controller
...
Business Context
Business owner
Risk owner
In PCI Network
Crown jewel
SLA & MTTR
...
Unified Context

Misconfigurations (Queries and Dashboard Templates)

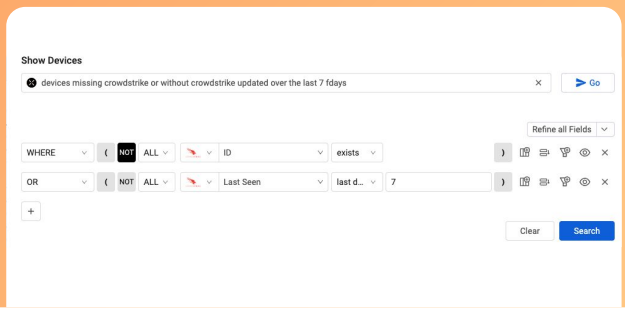
Out of the box, the Axonius discovery logic includes steps — aggregation, deduplication, normalization, and correlation — that can uncover gaps in security controls and misconfigurations such as:

- **Missing security controls**: By identifying a laptop reported by all your systems — CMDB, endpoint management, meeting client, and VPN client — but missed by your endpoint protection (EPP), you identify a gap in EPP coverage.
- **Gap in identity security posture:** By identifying users in an important department (reported by your HR), with admin rights, accessing a system without MFA (reported by your SaaS Apps), you identify a gap in identity coverage.
- **Shadow SaaS Apps**: By identifying a SaaS app purchased by your organization (reported by your expense system) or from your DNS monitoring, without SSO, MFA, or Identity Governance (reported by your Identity Provider), you identify SaaS applications missing critical security controls.

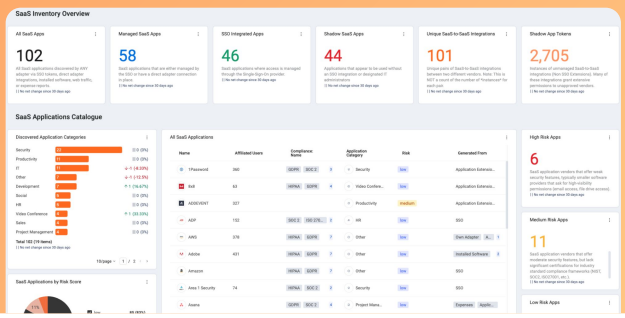
Queries identify assets with exposures including missing security controls (i.e. device missing crowdstrike) and misconfigurations (crowdstrike sensor installed but inactive). Queries can be presented in dashboards for tracking and used in subsequent CTEM steps: prioritization, validation, and mobilization.

Dashboard Templates — such as the SaaS Overview, Data Hygiene, and Security Posture dashboards — provide out of the box discoveries from Axonius in a dashboard format alongside baseline queries. The templates can be created from the Axonius Dashboard and tweaked to fit your needs.

Axonius Query Wizard:
Identifying gaps and misconfigurations in *Endpoint Protection* (i.e. Crowdstrike) coverage

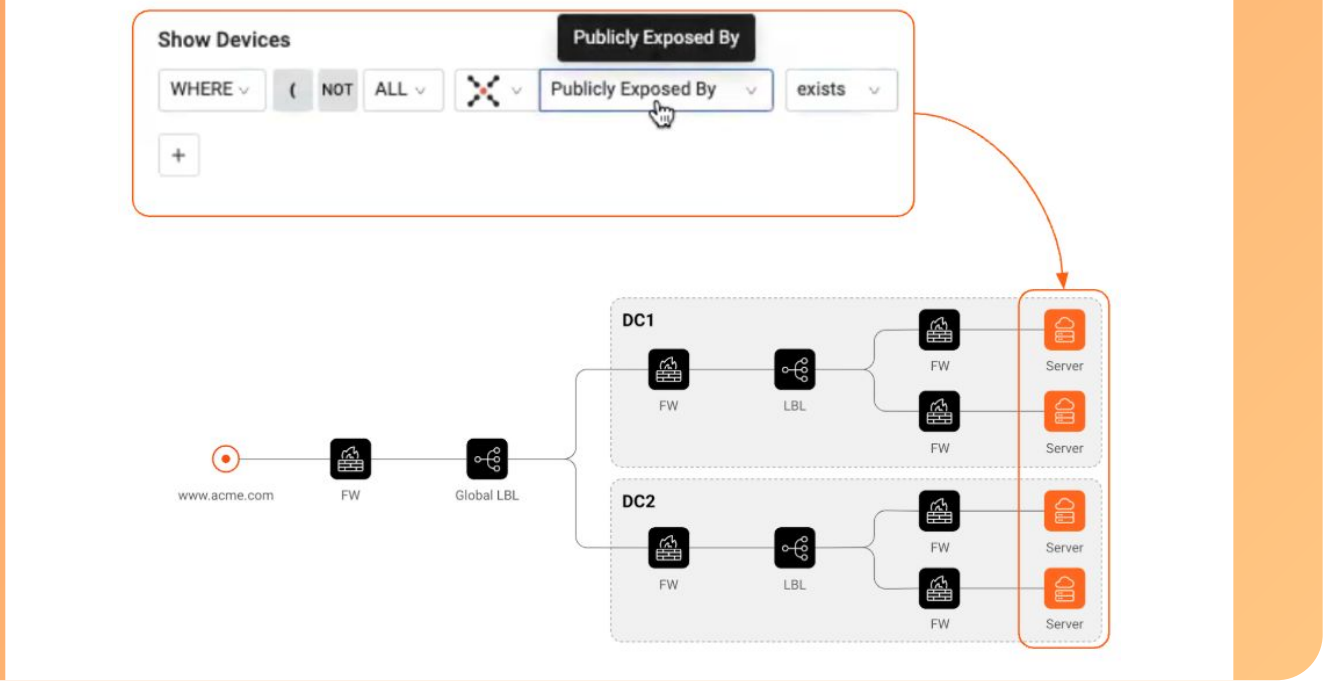


SaaS overview dashboard template displaying *exposures for SaaS Applications*



External to Internal mapping

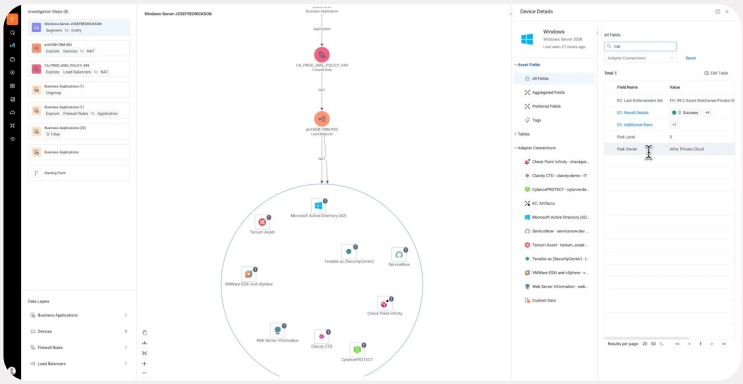
Throughout external to internal mapping, Axonius reviews the configuration of your network equipment — including your DNS, load balancers, firewalls, and subnets — to identify assets and exposures publicly exposed to external attackers.



The external to internal information is provided both in table format (mapping your configuration) and as a graph with additional asset context.

The identification through the network configuration — when compared to external scanning through the internet — provides three benefits:

- **high-fidelity signals** by leveraging your real attack surface as the baseline
- **identification of risk opaque to external scanners**, such as horizontal scale (adding new servers to increase production performance)
- **risk identification before incoming traffic is introduced.**



STEP 3:

Prioritization

GOAL

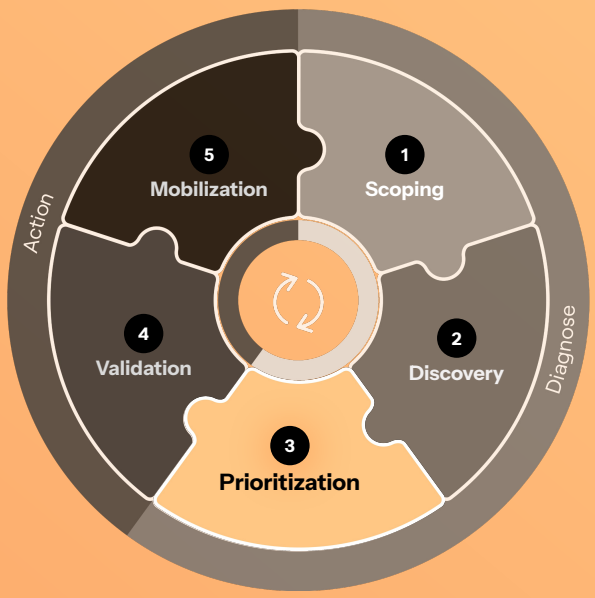
Focus Mitigation

Calculate exposure risk by factoring in business impact, exploitability, adversary behavior, and risk scores beyond CVEs/CVSS.

THE CHALLENGE

How to apply rigor and consistency amidst urgency?

- Issues and alerts lack business context and exploitability insights
- Often unclear ownership of the asset, the mitigation, and the result
- Internal and external SLAs often get in the way of risk-based prioritization



Prioritization with Axonius

Axonius supports prioritization by calculating the risk of your assets and exposures based on the security context (i.e. vulnerability CVE, technical score, threat intelligence feed data), asset context (i.e. asset state, status, and gaps), and business context (i.e. risk/business owner of the asset, crown jewel, in production, part of the PCI network). Axonius achieves prioritization through its unified context, risk score engine, and dashboards.

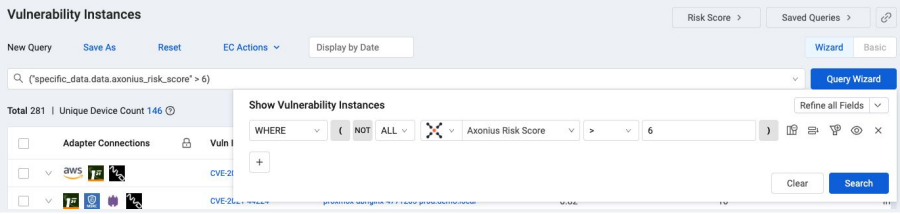
Unified Context

During Scoping and Discovery, Axonius collects and tracks the security context, asset context, and business context reported by your systems. This information is combined, correlated, and made available for every asset and exposure in the Axonius platform, making the unified context available for prioritization decisions across all components — including queries, risk engine, dashboards, workflows, and automations.

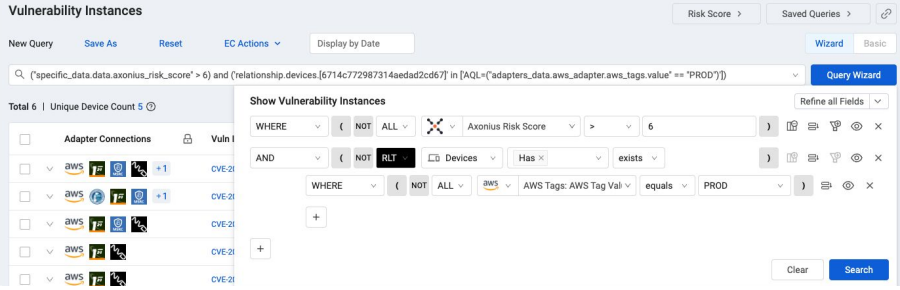
The Unified Context is the combination of Asset, Security and Business Context

Example:
Unified Context used in the platform:

Vulnerabilities with score higher than 6 (281 issues)



Vulnerabilities with score higher than 6 in AWS with a PROD tag (6 issues)

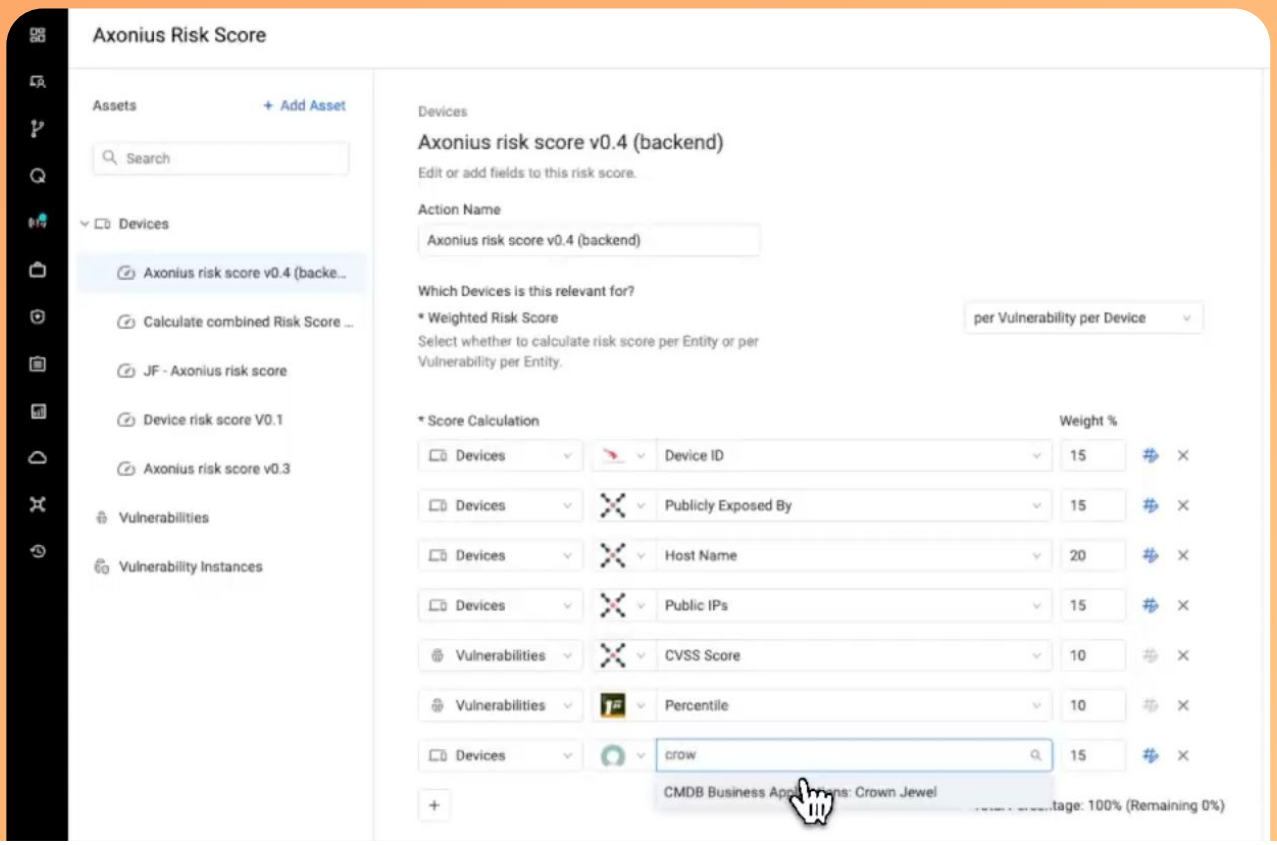


Risk Score Engine

The risk score engine quantifies the risk of assets and exposures based on the unified context. To calculate risk, organizations can either start from the Axonius-defined risk score or use their own logic based on their business characteristics.

Risk Score set up

Using security context (vulnerability scores and crowdstrike presence) alongside device context (hostname patterns, if the asset has public traffic from the internet), and business context (if asset is a crown jewel) to calculate risk.



The risk score helps organizations focus on exposures that require immediate attention and can also be used in subsequent steps to prioritize what exposures should go through validation and mobilization.

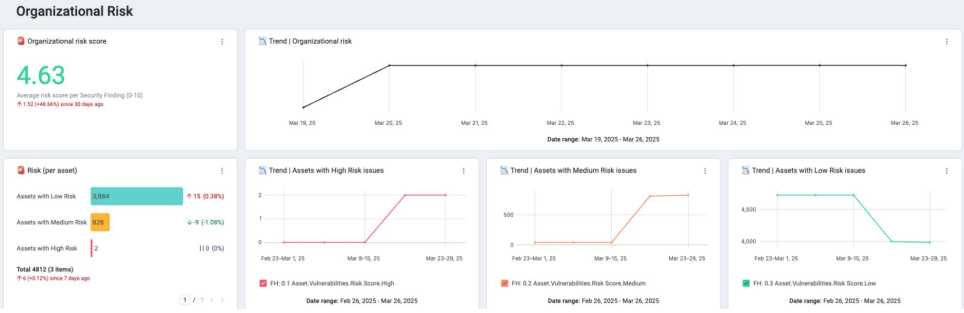
Dashboards

Dashboards leverage unified context and risk scores to surface CTEM prioritization in different ways.

Dashboards are also used in subsequent steps to track the validation and mobilization of prioritized exposures.

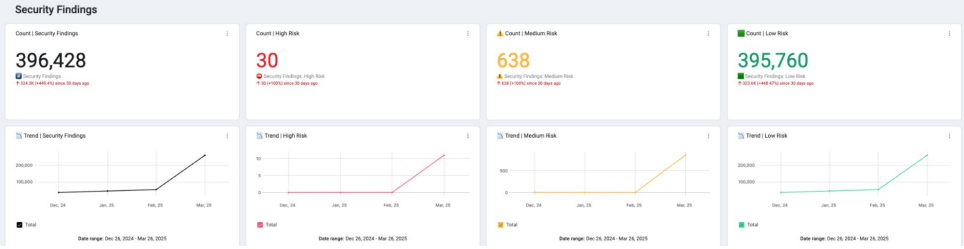
Organizational Risk

The overall view helps organizations track their current risk, historical performance, and risk in the attack surface broken by assets.



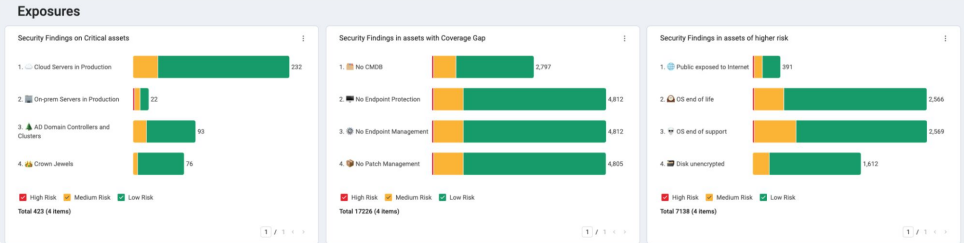
Security findings

Through the risk score, hundreds of thousands of security findings are segmented by risk, tracked historically, and associated with risk owners.



Explainability

The risk score and security findings can be surfaced and combined with asset views to drive discussions and prioritizations with key stakeholders



STEP 4:

Validation

GOAL

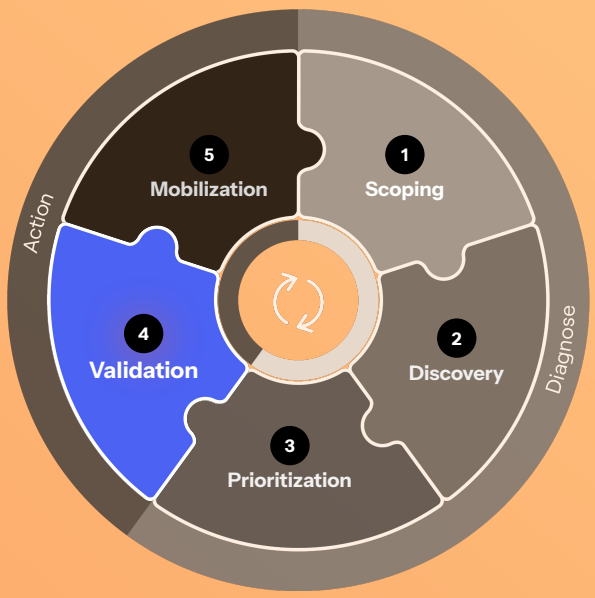
Confirm Exploitability

Test exposures with simulations, red teaming exercises, and attack path modeling to understand real world impact potential.

THE CHALLENGE

How to know what's real before it becomes real?

- Simulations are resource intensive and can fall to more pressing matters
- Full attack chains are often technically difficult to implement
- Testing can potentially disrupt production environments and teamwork



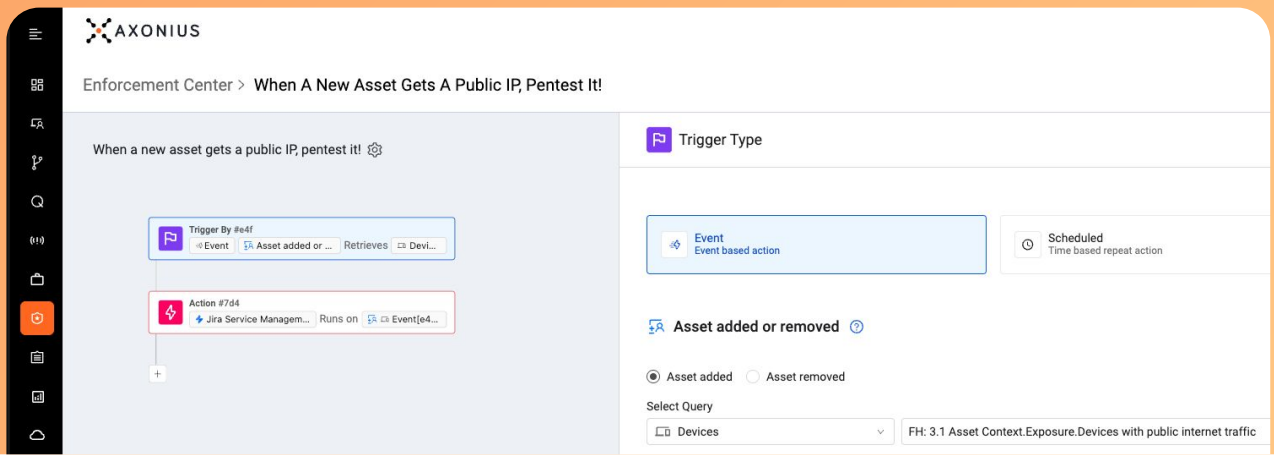
Validation with Axonius

While Axonius does not support native validation capabilities like Breach Attack Surface (BAS) or Pentest as a Service, the platform automates the start and coordination of the validation process through workflows.

Workflows

Axonius Workflows helps organizations automate actions whenever assets or exposures meet a condition. In the context of validation, workflows can be used for triggering a task run in your Breach and Attack Simulation (BAS) service for an automatic pen test or opening a ticket with your red team for manual pen testing with the targeted asset or exposure.

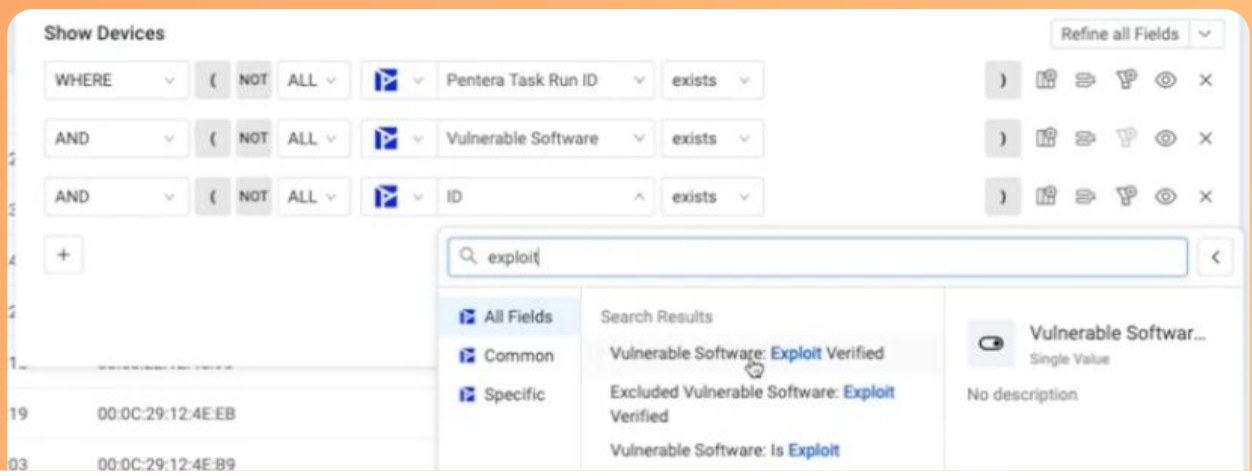
Validate exploit path when a new asset starts accepting *internet traffic*



Adapters

In the context of validation, Axonius adapters can confirm the completion of validation tasks from your red team and BAS services. Like any other data in Axonius, the data like exploit confirmations can be used across queries, risk prioritization, and to drive mobilization:

Using Exploit Verified from Pentera as *a validation confirmation signal*



Adapters can be used to bring confirmation signals not only from your own infrastructure (BAS tools) but also from other sources like Threat Intelligence Feeds.

STEP 5:

Mobilization

GOAL

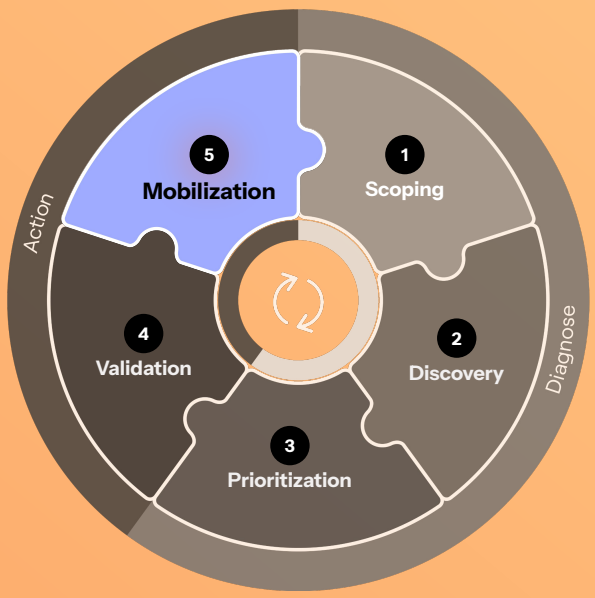
Take Action

Transform insights into streamlined remediation workflows coordinated across IT and Security operations teams.

THE CHALLENGE

How to break through issue fatigue to meet capacity?

- Even prioritized issues can be more volume than the team can handle
- Security & IT teams may still operate in mitigation silos
- Manual ticket-based remediation have slow lead and response times



Mobilization with Axonius

Axonius supports mobilization by identifying owners, triggering mobilizations through automation and tickets, tracking the remediation process, and validating if a remediation is effective.

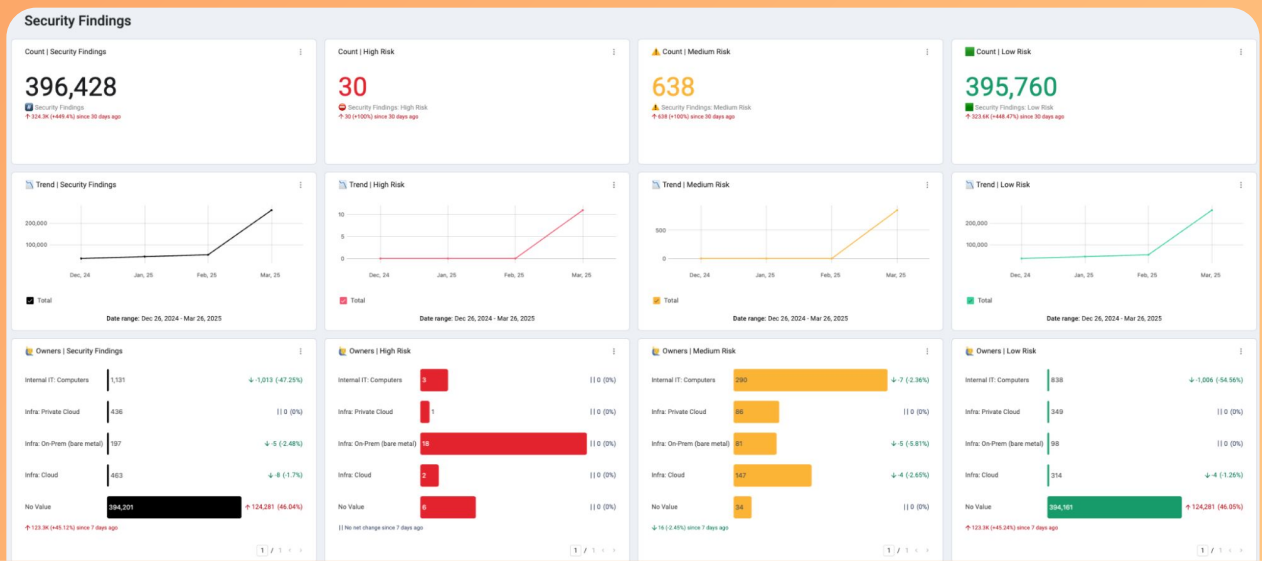
Axonius delivers mobilization through data, actions, workflows and enforcements, case management with ticket binding, and continuous Scoping and Discovery.

Data

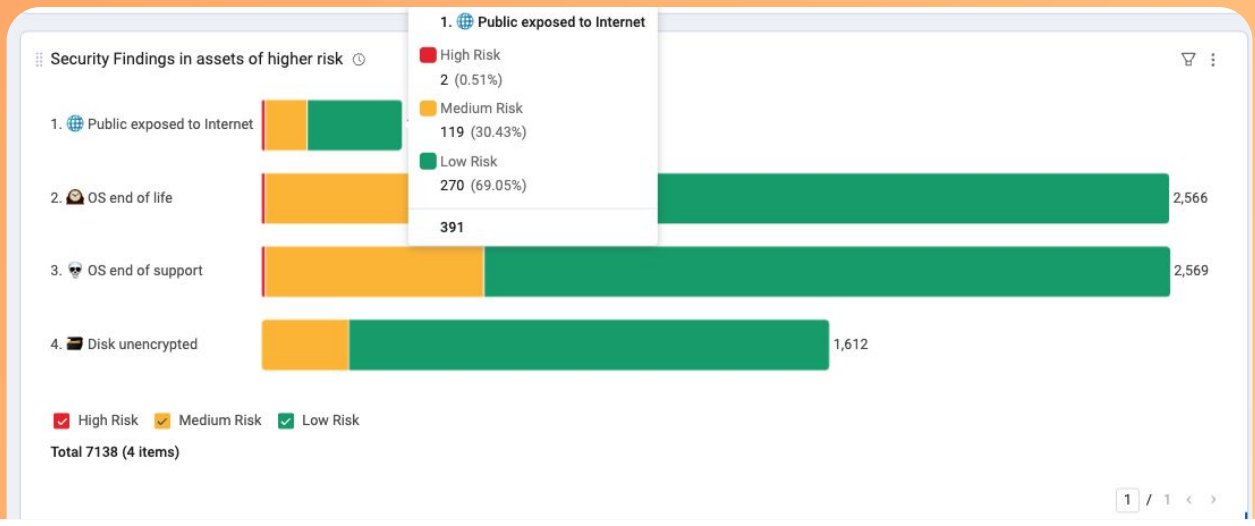
In the previous CTEM steps, Axonius collected accurate data across your assets and exposures with unified security, asset, and business context. This data is used as the basis for assigning owners, triggering, managing, and validating the mobilization across your attack surface.

- Unified Context is used to identify owners and conditions for triggering mobilization
- Queries are used to trigger workflows, ticket binding, and other remediation processes and later validate if a remediation was in fact implemented.
- Dashboards present data to manage the mobilization, ownership and the information for tracking, reporting, and carrying over conversations with other stakeholders in your company.

Dashboard displaying exposures *with risk owners*

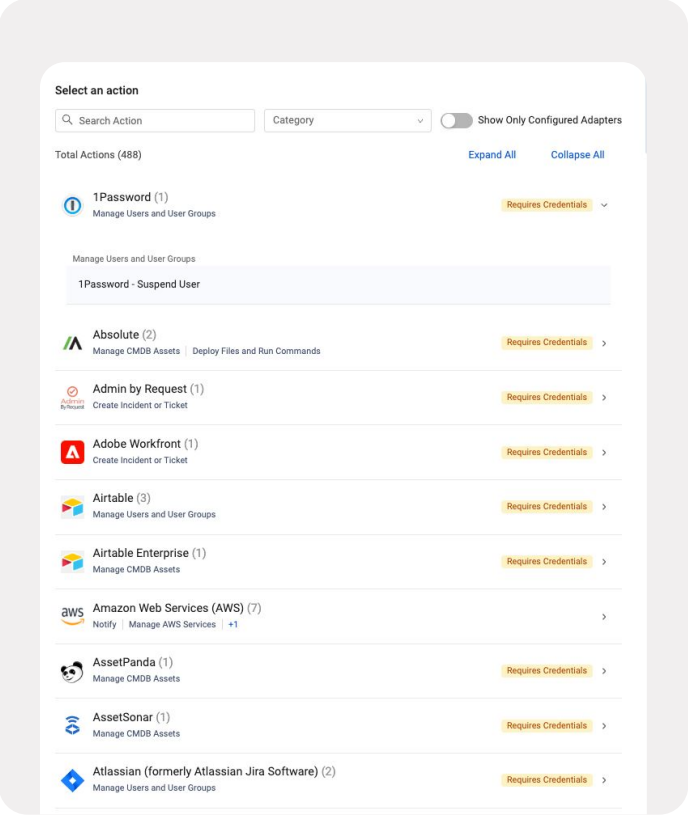


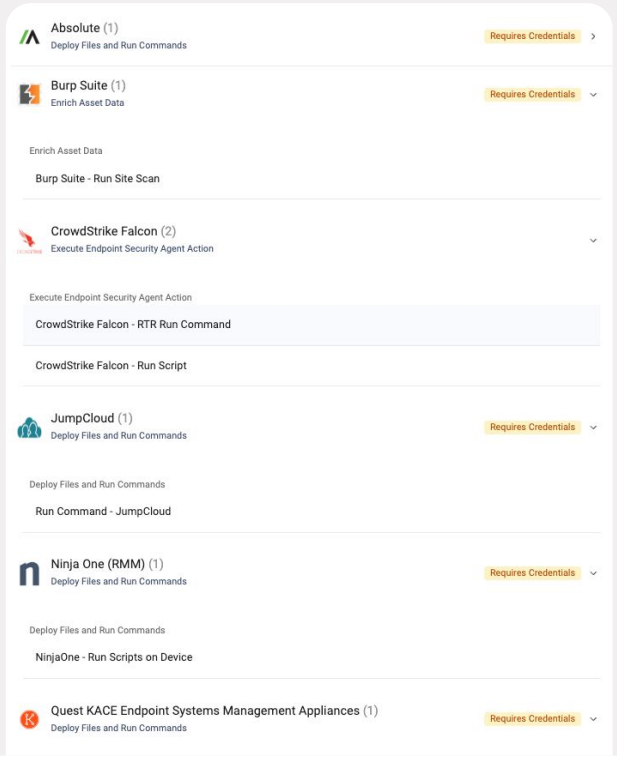
Dashboard displaying exposures of *high risk* on assets with an attack path from the internet



Enforcement Actions

Enforcement Actions are API-based integrations provided by Axonius to perform tasks in third-party systems. In the context of Mobilization, Enforcement Actions are used to automatically remediate third-party systems — through actions such as remote patch a workstation, deprovision a user, quarantine/isolate a laptop, or turn off a virtual machine — or that notify or mobilize teams to manually remediate exposures — through notifications and tickets. As of Mar-2025, Axonius supports 480+ actions. Actions can be triggered in three ways: through enforcements, workflows, or ticket binding.

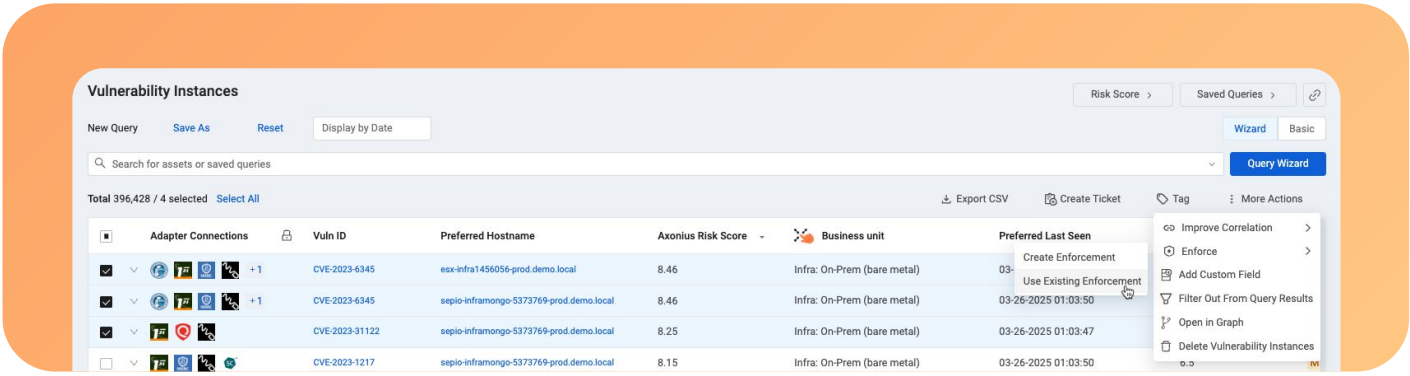




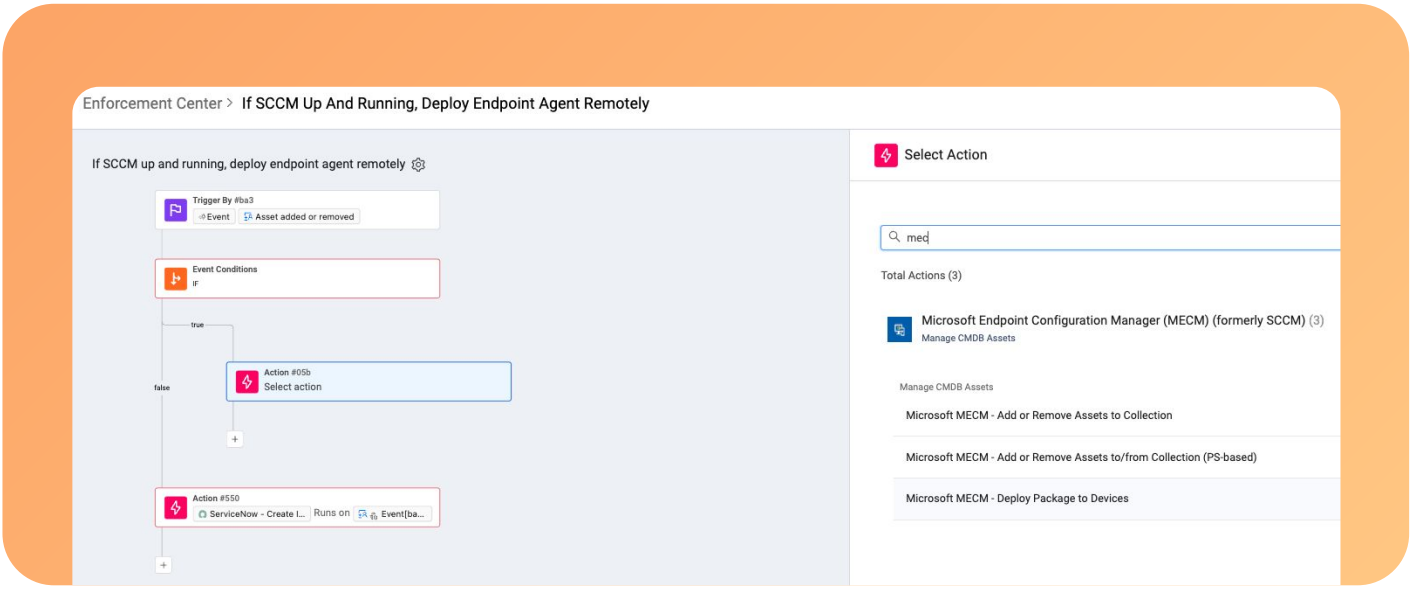
Workflows and Enforcements

Workflows and enforcements act as a trigger for mobilization in Axonius. By using queries or other triggers, you can define when the mobilization will happen and what actions should be performed.

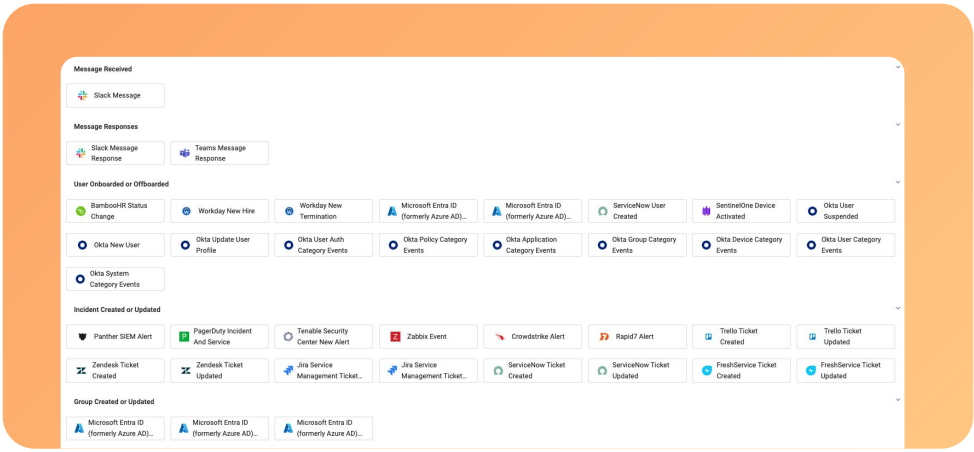
Enforcements provide a simple and easy way to mobilize. It's great for simple actions and can be triggered not only automatically, but also directly from the Axonius interface when a specific asset or exposure requires immediate mobilization.



Workflows are a new feature within the Axonius platform that expands enforcements with no-code, allowing you to add your own logic to the mobilization. Workflows work well when you need to change action based on logic — i.e. deploy an EPP agent only if the asset can receive remote commands via SCCM/MECM. Otherwise, open a ticket for manual remediation.

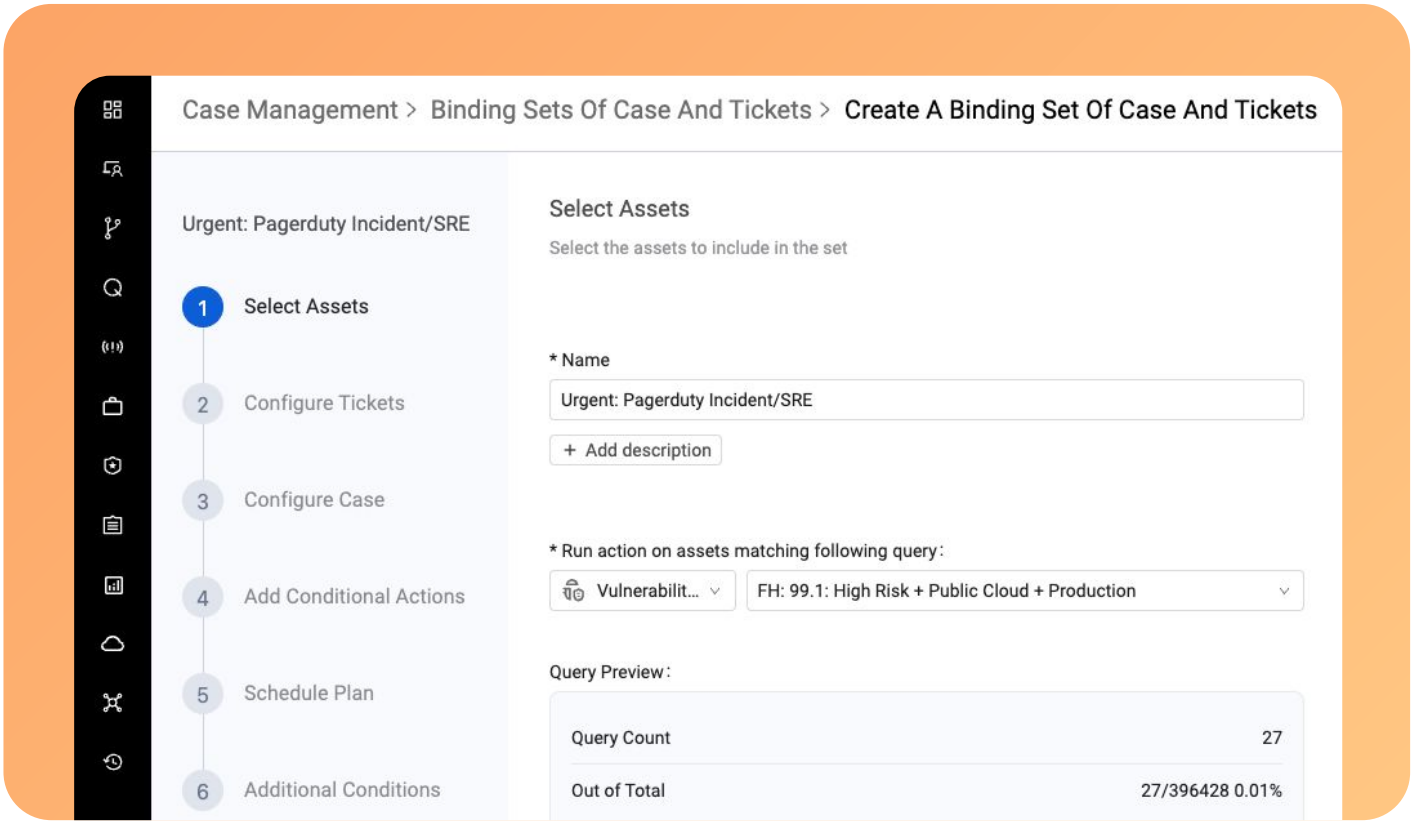


Workflows can also be triggered by events external to Axonius, such as when a slack message is received, an employment status change in HR, or a critical event is triggered by other solutions in your stack.

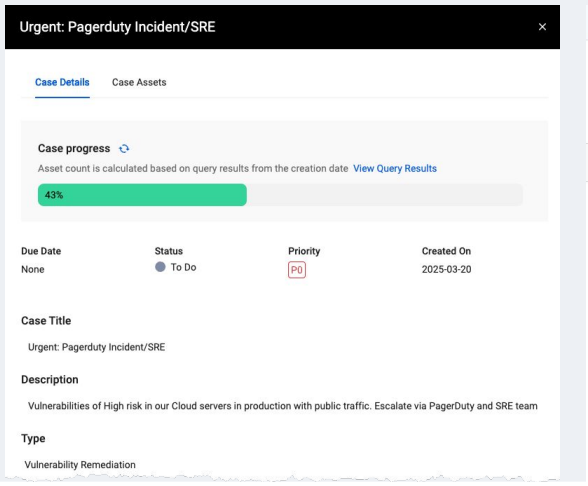


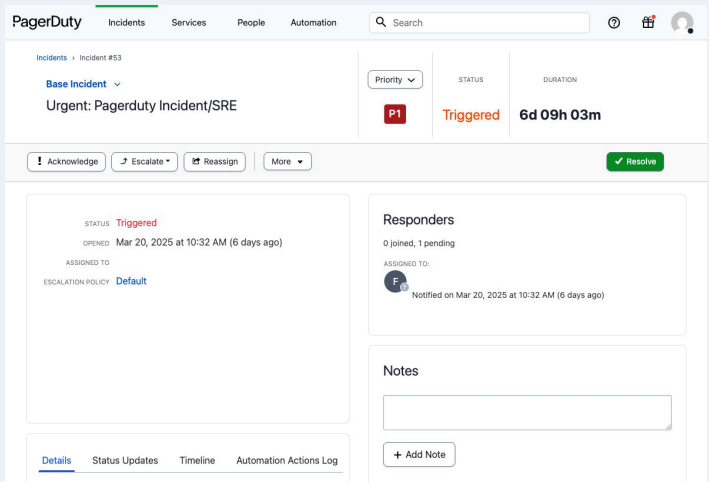
Case management and ticket binding

Case management and ticket binding serves as a trigger in Axonius for when you need to mobilize other teams across your organization through their ticket system of choice. Whenever a query is triggered, it uses your defined policy to mobilize the right team and ticket system — i.e. SRE team and PagerDuty, Internal IT and ServiceNow, Engineering and Jira, decide what ticket operation will be executed — i.e. create a new ticket or update an existing one, and create a case in Axonius to keep track of the ticket execution against your security MTTR and SLAs.



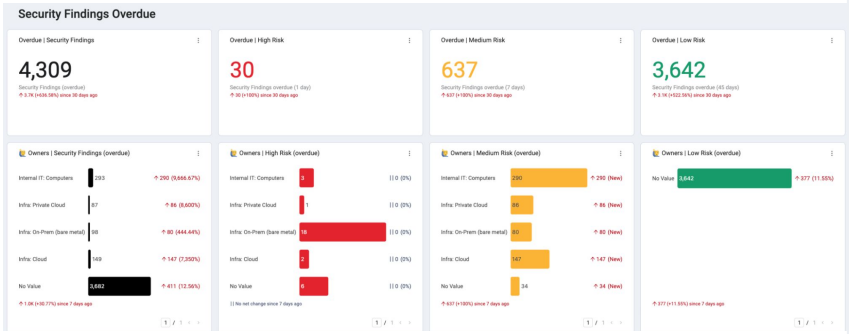
As ticket progresses, Axonius keeps track of what assets and exposures are fixed and the status of the associated ticket across different teams.





Through ticket adapters and dashboards, Axonius can continuously track the ticket progress and highlight tickets and cases overdue across different teams:

Exposures overdue across *different risk owners*



Exposures overdue across *the most critical assets*

Continuous Scoping, Discovery, and Prioritization

As highlighted in previous steps, Axonius continuously reassesses your Scope, Discovery, and Prioritization, as your attack surface changes and exposures are introduced or remediated. The Axonius findings are constantly reevaluated, updating the queries used to trigger mobilizations across all the features highlighted in this step. That provides many benefits including:

- **Write once, always enforce**: Your mobilization is triggered whenever new assets or exposures are identified by a query.
- **Re-enforce as risk is reintroduced**: Mobilizations are re-triggered whenever asset risk or exposures are reintroduced to your attack surface.
- **Closed loop remediation**: Mobilizations are re-triggered if a ticket is closed but the issue is not solved

Getting Started with *CTEM*

As an organization-wide approach, CTEM requires a holistic strategy — inclusive of processes, technologies, and people — and time to be successful.

Through the Implement a Continuous Threat Exposure Management (CTEM) Program research, Gartner provides a complete approach for implementing CTEM in their enterprises.

To increase your chances of a successful CTEM implementation, we recommend breaking down the CTEM adoption into incremental steps with milestones and wins to build momentum, avoid scope creep, and identify and address adoption challenges early and often.

01 Start with visibility

Successful CTEM programs are rooted in accurate and up-to-date view of assets and exposures. On the opposite side, a program without confidence in visibility (and without a clear management of expectations) may create the false sense of safety or mismatch the expectation of stakeholders. By investing in a strong visibility (scoping and discovery), you set the foundation for a successful program.

02 Enable an agile CTEM implementation with quick feedback loops

By investing in the frequency in which the CTEM process is executed (i.e. running full cycles at least once a day), you reduce your mean time to recognize and fix issues while at the same time creating a quick feedback loop for tests, ideation, continuous improvements, and automation. In other words, you create agility and adaptability with your program, avoiding analysis paralysis.

03 Improve Prioritization, Validation, and Mobilization through repeatable iterations

With strong visibility and quick feedback loops, you have a strong launchpad for prioritization, validation, and mobilization improvements. These phases can start with your existing policies, and rapidly evolve based on your learnings from each CTEM cycle. Initial cycles and improvements will yield more dramatic impact and results and gradually reach a point of diminishing returns.

04 Look for Proactive/Preemptive actions and Automation opportunities

While CTEM does not explicitly list preemptive/proactive actions or automations as distinct steps in its process, both are deeply embedded in the CTEM approach. When implementing CTEM, you should take an intentful approach on finding opportunities for implementing these actions.

Examples include (but are not limited to):

Preemptively reduce the attack surface footprint and save costs with asset hygiene (i.e. retire assets no longer in use) and hardening (i.e. remove software not in use in existing assets or harden its configuration).

Proactively reduce risks by implementing strong security controls processes like patch management and MFA.

Find opportunities to implement automations to reduce the number of tickets and dependence on humans to complete critical work.

Getting Started with *Axonius*

The Axonius platform is designed and built with architectural principles to help your organization get up and running fast.

- Deployment in Hours
- 1,000+ pre-built Integrations
- No agent or network proxy required
- Connects to Solutions Using Adapters

Through our integration network and adapters that do not require agents or network proxies, you can quickly integrate with all your systems to find assets and exposures very fast.

On average, our customers take 14 days to go into production with continuous growth across assets, automation, and return on investments.

14 days
to go production

57%
Assets secured growth (in 6 months)

90%
Remediation automation growth (in 6 months)

The Axonius adoption steps align directly with the five steps of the CTEM approach.

- **Scope and Discovery:** By integrating your adapters for assets and exposures, you immediately get immediate benefits of scoping and discovery across your entire attack surface across on-prem, public cloud, and private clouds.
- **Prioritization**: From there, you can leverage risk scores, queries, and insights to prioritize the exposures that matter most.
- **Validation and Mobilization:** Once assets and exposures are and prioritized, our customers immediately adopt enforcements, workflows, and case binding for both validation and mobilization. (On average, our customers grow these actions in about 90% over the 1st 6 months)

Continuous on day one:

With scoping and discovery running continuously from day one, Axonius implements a repeatable process foundational for establishing and improving your CTEM approach, building a virtuous cycle.

This continuous approach provides many organizations a linchpin for their security strategy:

Built by security. Loved by security

epiq

"(Axonius) drives our automation, discovery, and key portions of our strategy. Axonius provides the luxury of being able to evaluate where we stand by quickly visualizing our gaps as we build out our cybersecurity program."

Alyssa Miller | CISO
axonius.com/resources/epiq-follow-up-case-study

cimpress · Schneider Electric · AB InBev · Bed Bath & Beyond | overstock · Blackhawk Network · Rakuten Mobile · The New York Times · News Corp · coupa

To get started with Axonius for CTEM, contact us and schedule a demo and a conversation with our team.

Schedule a demo

APPENDIX A:

References

Axonius' documentation:

- Axonius Adapters
- Axonius Adapter List
- Asset Types
- Discovery Cycle
- Discovery Schedule Settings
- Real-time Adapters
- Discovery retention
- Vulnerability Enrichments
- NIST National Vulnerability Database (NVD)
- CISA Known Exploited Vulnerabilities (KEV)
- Exploit Prediction Scoring System (EPSS)
- Microsoft Security Response Center (MSRC)
- Queries
- Dashboard Templates
- Enforcement Actions
- Enforcements
- Workflows
- Axonius Exposures
- Vulnerability Instances
- Risk Scoring
- Publicly Exposed By

Other References:

- Continuous Threat Exposure Management (CTEM): A Guide to Proactive Cybersecurity
- Ditch the Checkboxes: A Guide to Risk-Based Vulnerability Management
- Is CTEM the New Zero Trust — Virtual Webinar
- How To Strengthen Vulnerability Risk Management With Remediation Prioritization, Forrester
- How To Implement a Risk-Based Vulnerability Management Methodology, Gartner, 20 April 2023
- The Top 5 Elements of Effective Vulnerability Management, Gartner, 9 January 2024
- Implement a Continuous Threat Exposure Management (CTEM) Program, Gartner, 11 October 2023

APPENDIX B:

Feature Matrix: *Axonius and CTEM*

	CTEM Steps				
Axonius features and documentation	Scoping	Discovery	Prioritization	Validation	Mobilization
Adapters:					
Assets	✖				
Vulnerabilities		✖			
Cloud Exposures		✖			
Application Development Exposures		✖			
Tickets					✖
Threat Intelligence		✖			
Breach Attack Simulation	✖	✖		✖	
Asset Types	✖				
Discovery					
Logic/lifecycle	✖	✖			
Continuous Discovery	✖	✖			
Real-time Discovery	✖	✖			
Retention	✖	✖			
Static Analysis and Enrichments		✖	✖		
Exposures		✖	✖		
External to Internal		✖	✖	✖	✖
Unified Context		✖	✖		
Queries		✖	✖	✖	✖
Dashboards			✖		✖
Dashboard Templates			✖		✖
Risk Score			✖	✖	✖
Enforcement Actions				✖	✖
Enforcements				✖	✖
Workflows				✖	✖
Case Management and Ticket Binding				✖	✖