Axonius

Ten Questions *Every Cybersecurity Team Must Ask* (and get answers to) About Cyber Asset Management

A Comprehensive Guide for Security Pros

March 2025

Contents

Introduction

Understanding your organization's cyber assets isn't just good practice, it's vital to business success. This guide explores the ten most critical questions Chief Information Security Officers (CISOs) and other security leaders should ask about their cyber asset management approach, framed through real-world scenarios and consequences.

The Asset Visibility Crisis

Imagine receiving an urgent alert from your security team. An unknown device has access to sensitive data on your network. Your team scrambles to respond, but they're fighting blind. Which device is it? Who owns it? What security controls should be in place? These questions may seem basic but could become paralyzing in the wake of an incident.

The Asset Explosion

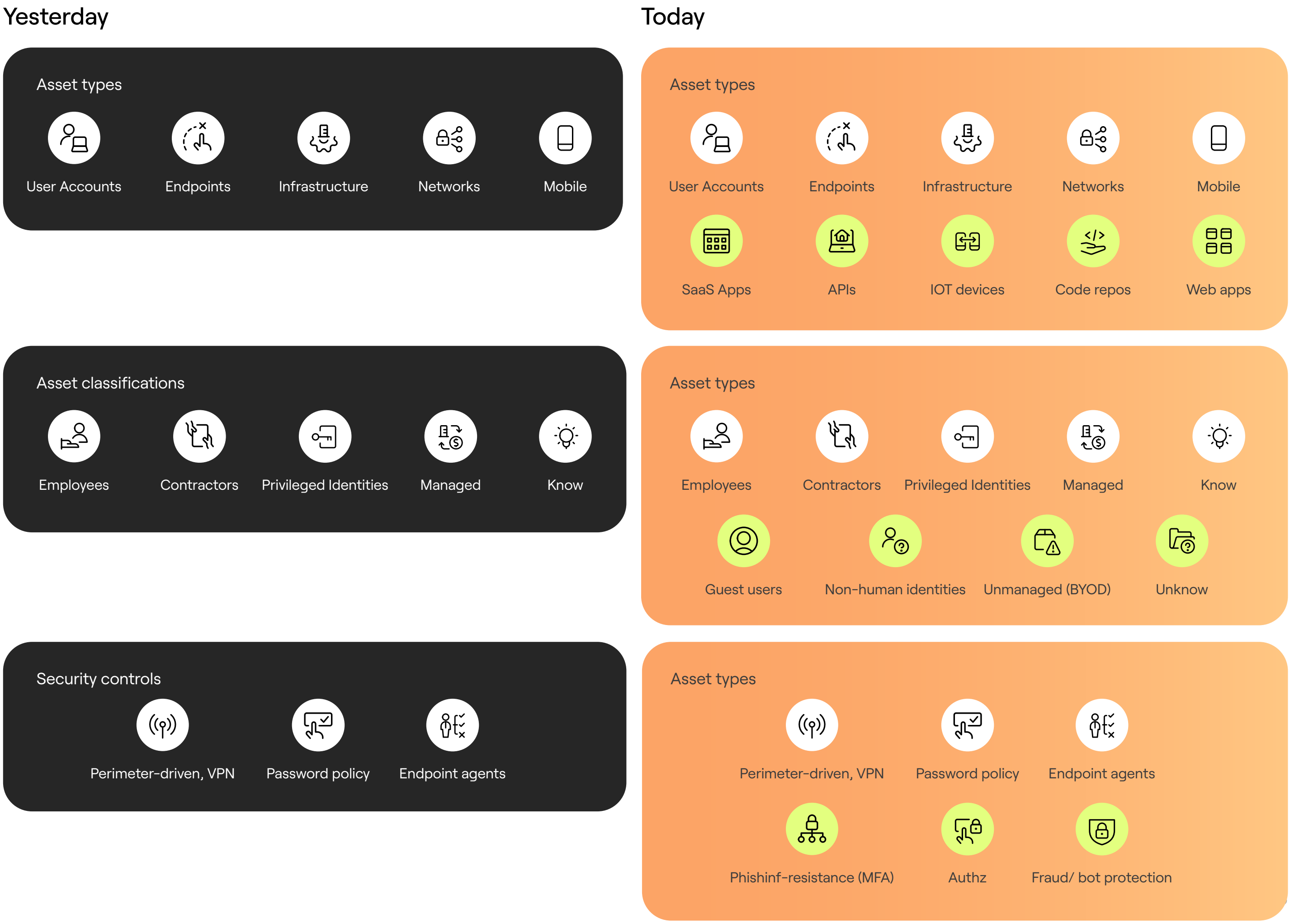
The challenge of managing cyber assets is hardly a new one – to put it simply, any organization that has an expanding set of assets to manage and secure needs to have a strategy around how to do that. But, that's easier said than done.

As businesses evolve, so does the scope of what you need to manage. Cloud infrastructure, mobile devices, laptops, BYOD, identities, SaaS apps – it's all fair game. The challenge is more about prioritizing cyber asset management over the many other security needs a company typically has.

Today's Reality

Organizations typically rely on a patchwork of solutions:

- Spreadsheet and more spreadsheets which become immediately outdated
- Point solutions with conflicting data
- CMDBs that do not discover unknown/ unmanaged assets
- Ad-hoc processes that don't scale



Yesterday

Asset types: User Accounts, Endpoints, Infrastructure, Networks, Mobile

Asset classifications: Employees, Contractors, Privileged Identities, Managed, Know

Security controls: Perimeter-driven, VPN, Password policy, Endpoint agents

Today

Asset types: User Accounts, Endpoints, Infrastructure, Networks, Mobile, SaaS Apps, APIs, IOT devices, Code repos, Web apps

Asset types: Employees, Contractors, Privileged Identities, Managed, Know, Guest users, Non-human identities, Unmanaged (BYOD), Unknow

Asset types: Perimeter-driven, VPN, Password policy, Endpoint agents, Phishinf-resistance (MFA), Authz, Fraud/ bot protection

The Questions That Keep *CISOs Awake*

Devices

Question 1: Is the device known and managed?

The Stakes

The National Institute of Standards and Technology (NIST) defines unmanaged as: “A device inside the assessment boundary that is either unauthorized or, if authorized, not assigned to a person to administer.” Almost 7 in 10 organizations admit they have experienced at least one cyberattack started by exploiting an unknown, unmanaged, or poorly managed internet-facing asset (JupiterOne). When Colonial Pipeline suffered its devastating breach, the attack vector was an unknown VPN device that lacked multi-factor authentication.

The Challenge

With the rise of IoT, BYOD, and shadow IT, the distinction between “known” and “unknown” devices has never been more confusing. Organizations struggle to:

- Maintain accurate real-time device inventories
- Track device management status across multiple systems
- Identify shadow IT and rogue devices
- Ensure consistent security coverage

Critical inputs:

1. Real-time inventory of all devices touching your corporate resources
2. Endpoint agent coverage
3. Anomalous device behavior (e.g. random access times)
4. Speed in identifying and responding to unknown or unmanaged devices

Question 2: Who owns the device and where is it located?

The Stakes

The exploitation of device location data can reveal details about the number of users in a location, user movements, and can expose unknown associations between users and locations. A single device on the wrong network segment could provide attackers with a foothold into your crown jewels.

The Challenge

Modern enterprises must track devices across:

- Multiple (sometimes hundreds or thousands) of geographic locations
- Multiple network segments
- Cloud environments
- Remote and hybrid work setups
- IoT deployments

Critical inputs:

1. User ownership (where applicable)
2. Enforcement of device posture and location-based access policies
3. Devices that pose the highest risk (specific to vulnerabilities and gaps in security posture, e.g. no mobile device management agent)?

Question 3: What type of device is it?

The Stakes

Misidentifying device types is like playing Pin the Tail on the Donkey with your security strategy. Entertaining, but misguided. Only 17% organizations can clearly identify and inventory a majority (95% or more) of their assets.

The Challenge

Modern enterprises must identify and manage:

- Traditional endpoints (laptops, desktops, servers)
- Virtual machines, including ephemeral instances
- IoT devices (from smart thermostats to that mysterious device in the break room)
- Cloud assets that appear and disappear like digital ninjas

Critical inputs:

1. Device ownership
2. Security controls for specialized devices that do not have a human owner (e.g. devices that run scripts or bots)
3. Security controls on production vs test environments

Software

Question 4: Is core software updated?

The Stakes

Verizon's 2024 Data Breach Investigations Report found that ransomware attacks originating from unpatched vulnerabilities had far more severe consequences, including higher ransom demands and longer recovery times. The average time to exploit a new vulnerability? A mere 48 hours, hardly enough time to finish your coffee, let alone manually patch your entire infrastructure.

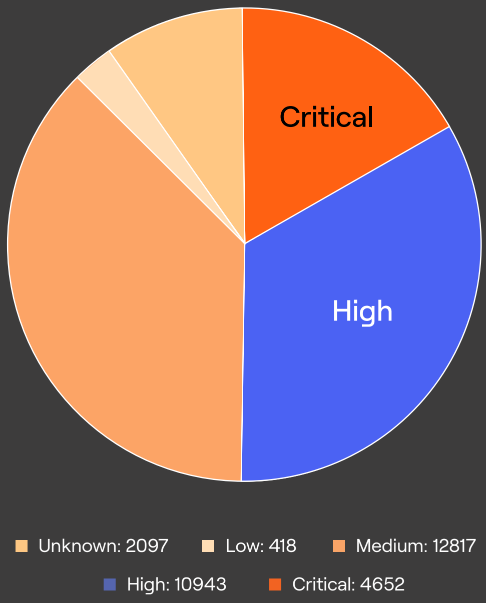
The Challenge

Organizations struggle with:

- Identifying the critical vulnerabilities that are actually critical in the context of your business
- Tracking multiple operating system versions
- Balancing security updates with business continuity

Critical inputs:

1. Categories of asset criticality (e.g. internet devices are more vulnerable than in-network devices)
2. Establishing a framework for identifying critical vulnerabilities
3. Tracking MTTD (mean time to detect) and MTTR (mean time to respond)



30k+ CVEs

11k+ High CVE score

5k+ Critical CVE score

Which CVEs *actually matter* to our business?

Question 5: How are you identifying unauthorized software or apps?

The Stakes

Managing Shadow IT (and more recently, Shadow AI) comes down to having a plan in place for awareness. Gartner estimates that by 2027, 75% of employees will acquire, modify or create technology outside IT's visibility – up from 41% in 2022.

The Challenge

Security teams must contend with:

- Balancing security vs usability
- Data leakage as a result of shadow IT
- Enforcing security controls on apps unmanaged by IT (e.g. Single Sign-On and Multi-Factor Authentication)

Critical inputs:

1. SaaS app inventory
2. Tracking software compliance, especially for SaaS apps
3. Identifying unauthorized installs
4. Identifying the frequency at which unmanaged apps are being accessed

Cloud Infrastructure

Question 6: Which users have unchecked access policies?

The Stakes

Engineering and DevOps teams spin up cloud workloads on a monthly, weekly, and even daily basis. While the cloud infrastructure under the purview of IT may consistently receive the correct security policy enforcements, these ephemeral instances, unmanaged by IT, likely do not. CrowdStrike reported a 75% increase in cloud-based intrusions from 2022 to 2023, and the problem is likely to grow as, per Gartner, cloud computing is expected to become a business necessity by 2028.

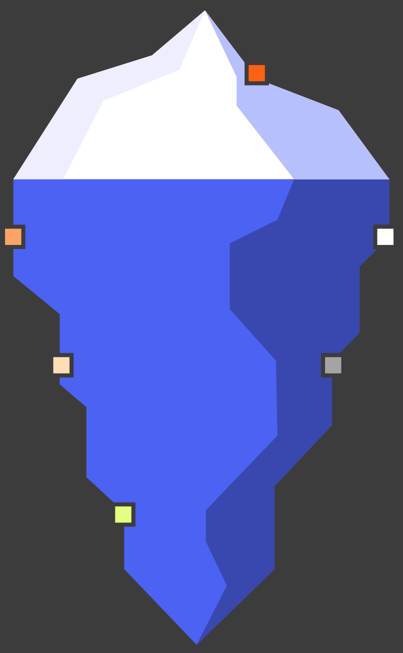
The Challenge

Security teams must balance:

- Policy enforcement vs day-to-day engineering operations requirements
- Keeping up with cloud misconfigurations
- Identifying which types of cloud infrastructure is the most vulnerable to exploit

Critical inputs:

1. The frequency of ephemeral cloud instance builds
2. Infrastructure that does and does not receive security policy
3. Frequency of access/last access time (to understand when to decommission)



🟥 Severity

Cloud instances managed by devs

🟧 Asset criticality

Identifying a high-risk vuln on a public facing vs development server

🟨 Does the vulnerability impact an easy entry point for threat actors?

Identifying a high-risk vuln on a public facing vs development server

🟩 Exploitability

Probability of threat actors exploiting the vulnerability

⬜ Assets created and managed outside security team

Cloud instances managed by devs

◼ Business context

How quickly does the vuln need to be remediated to adhere to our organizational security policies?

Identities

Question 7: Which users have unchecked access policies?

The Stakes

We've all read it - compromised credentials continue to be a prominent, if not the primary, attack vector in breaches. Verizon's 2024 Data Breach Investigation Report tells us that compromised credentials continue to be the weakest link in securing against breaches.

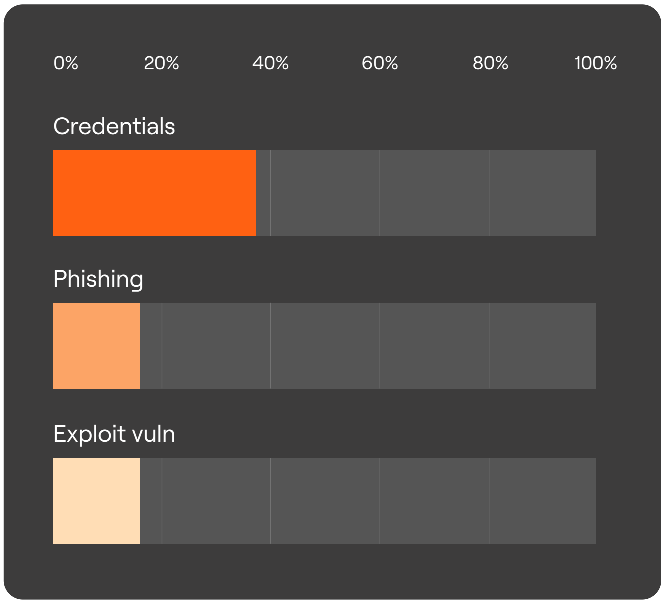


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

The Challenge

Managing a proliferation of identities and access over time:

- New types of users - including non-human accounts
- Users accumulate permissions over time, many of which are not granted via least privilege
- Disjointed mover, leaver, joiner processes between HR, IT, and Security
- Accounts persist beyond their needed lifecycle (orphaned accounts)

Critical inputs:

1. Categorizing account types - human (employee, contractor, contingent worker etc) vs non-human (service accounts, devices, bots)
2. Anomalous user access activity
3. Account last active times
4. Permissions required vs permissions granted; roles required vs roles granted

Question 8: Do I Have Users with Devices Not Seen in the Past 30 Days?

The Stakes

Gartner predicts that by 2026, 25% of IAM leaders will be responsible for both cybersecurity and business results, operating from the C-suite as chief identity officers (CIDOs). Identity has quite a broad scope - and that includes device identity.

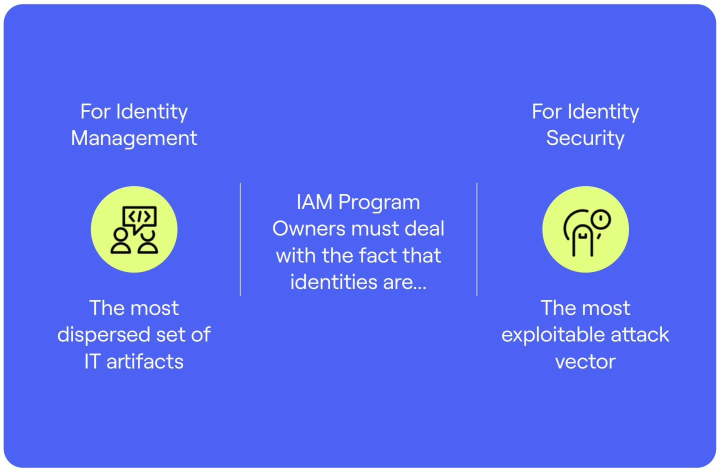
The Challenge

Security teams must track:

- Remote and hybrid worker devices
- Contractor devices
- Short-term assets deployed for temporary projects
- User to device ownership

Critical inputs:

1. Total # of managed endpoints in the organization
2. Total # of BYOD devices in the organization
3. Offboarding process for devices
4. Identifying lost and/or stolen devices


For Identity Management
The most dispersed set of IT artifacts
IAM Program Owners must deal with the fact that identities are...
For Identity Security
The most exploitable attack vector

Question 9: Do we have users that have turned off their endpoint protection agent?

The Stakes

Disabling security agents is kind of like disabling your smoke detector - it can be super annoying, but it is also a form of insurance policy. In some instances, endpoint protection becomes disabled as a result of a malfunctioning agent. In other instances, users find a way to circumvent policy and intentionally disable endpoint protection agents.

The Challenge

Security teams must manage:

- User circumvention of security controls
- Performance versus security balancing
- Shadow IT proliferation
- Limited visibility into agent status

Critical inputs:

1. Discovering devices with disabled endpoint protection agents (across any OS)
2. Monitoring endpoint protection agent health
3. Process to re-enabled endpoint protection agents

Security Policies

Question 10: What percentage of our cyber assets comply with organizational security policies?

The Stakes

While the average cost of compliance is around $5.5 million, the cost of non-compliance is almost $15 million. Beyond the financial impact, policy gaps can create substantial risks for security breaches, brand damage, and litigation.

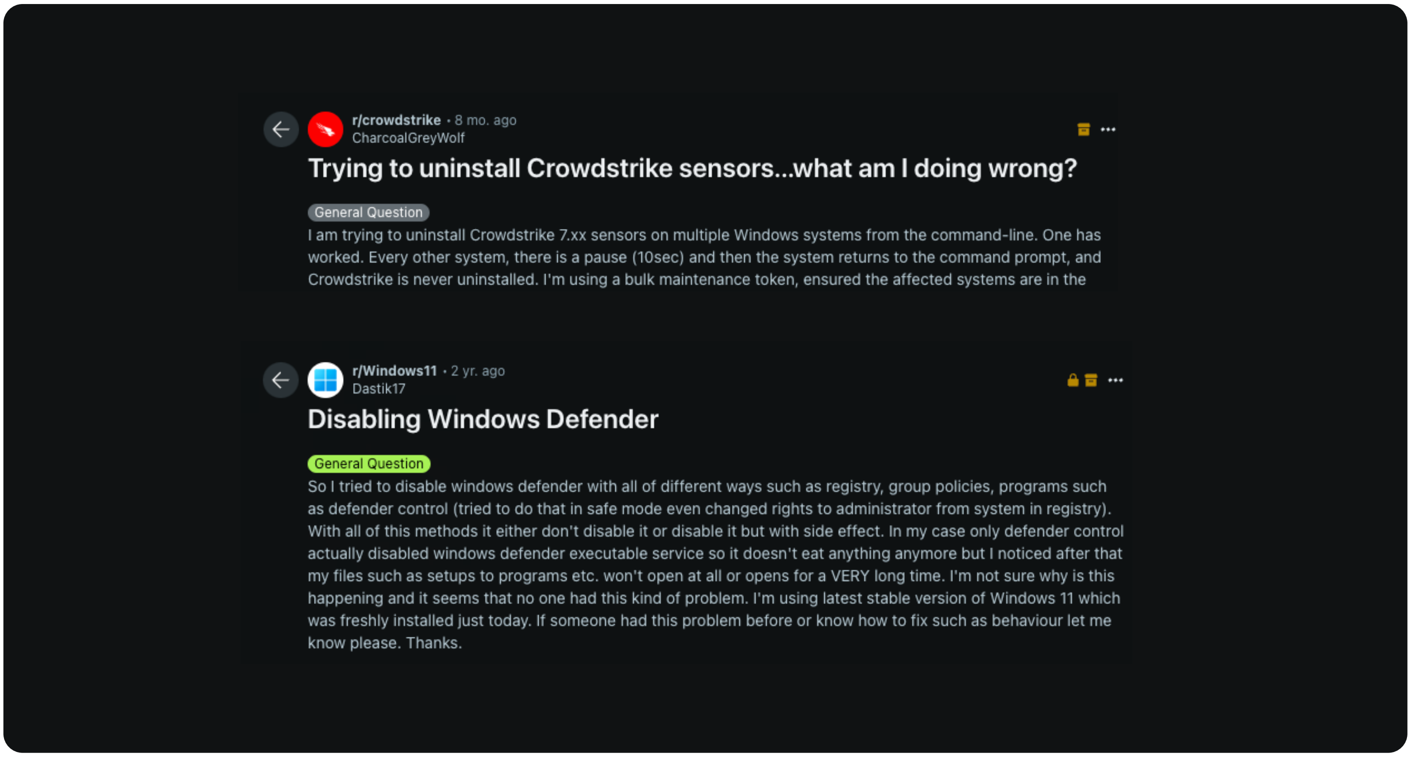
The Challenge

Managing a proliferation of identities and access over time:

- Multiple compliance frameworks (NIST CSF 2.0, ISO 27001, etc.)
- Industry-specific regulations (GDPR, CCPA, PCI DSS 4.0, etc.)
- Global privacy requirements
- Internal security policies

Critical inputs:

1. Process for automating evidence collection for audits
2. Tracking and enforcing security baselines



r/crowdstrike • 8 mo. ago
CharcoalGreyWolf

Trying to uninstall Crowdstrike sensors...what am I doing wrong?

General Question

I am trying to uninstall Crowdstrike 7.xx sensors on multiple Windows systems from the command-line. One has worked. Every other system, there is a pause (10sec) and then the system returns to the command prompt, and Crowdstrike is never uninstalled. I'm using a bulk maintenance token, ensured the affected systems are in the

r/Windows11 • 2 yr. ago
Dastik17

Disabling Windows Defender

General Question

So I tried to disable windows defender with all of different ways such as registry, group policies, programs such as defender control (tried to do that in safe mode even changed rights to administrator from system in registry). With all of this methods it either don't disable it or disable it but with side effect. In my case only defender control actually disabled windows defender executable service so it doesn't eat anything anymore but I noticed after that my files such as setups to programs etc. won't open at all or opens for a VERY long time. I'm not sure why is this happening and it seems that no one had this kind of problem. I'm using latest stable version of Windows 11 which was freshly installed just today. If someone had this problem before or know how to fix such as behaviour let me know please. Thanks.

Taking Back Control of your *Cyber Assets*

Identifying, managing, and remediating your cyber assets today requires a shift in approach. Rather than adding more tools to an already complex environment, organizations need a unified solution that can:

- Aggregate and normalize data from existing security and management tools
- Provide real-time visibility across all asset types
- Automate policy enforcement and remediation
- Deliver actionable insights to empower security decisions

The Power of Integration

A comprehensive solution transforms how organizations understand and secure their assets by:

- Integrating with all your existing enterprise technologies (e.g. Crowdstrike, Okta, Microsoft Entra ID, ServiceNow, Qualys etc) to gather and correlate asset data
- Enabling flexibility in enforcing remediation either automatically or point-in-time
- Identifying misconfigurations and exposures before threat actors do
- Maintaining continuous compliance with regulatory requirements

Today

Limited asset visibility

Manual efforts for asset correlation

Disparate asset data across tools

Goal

✓ Comprehensive understanding of attack surface

✓ One go-to platform for asset visibility and attack surface management

✓ Contextualized, prioritized insights for remediation

Axonius: Bring Truth to Action with *Asset Intelligence*

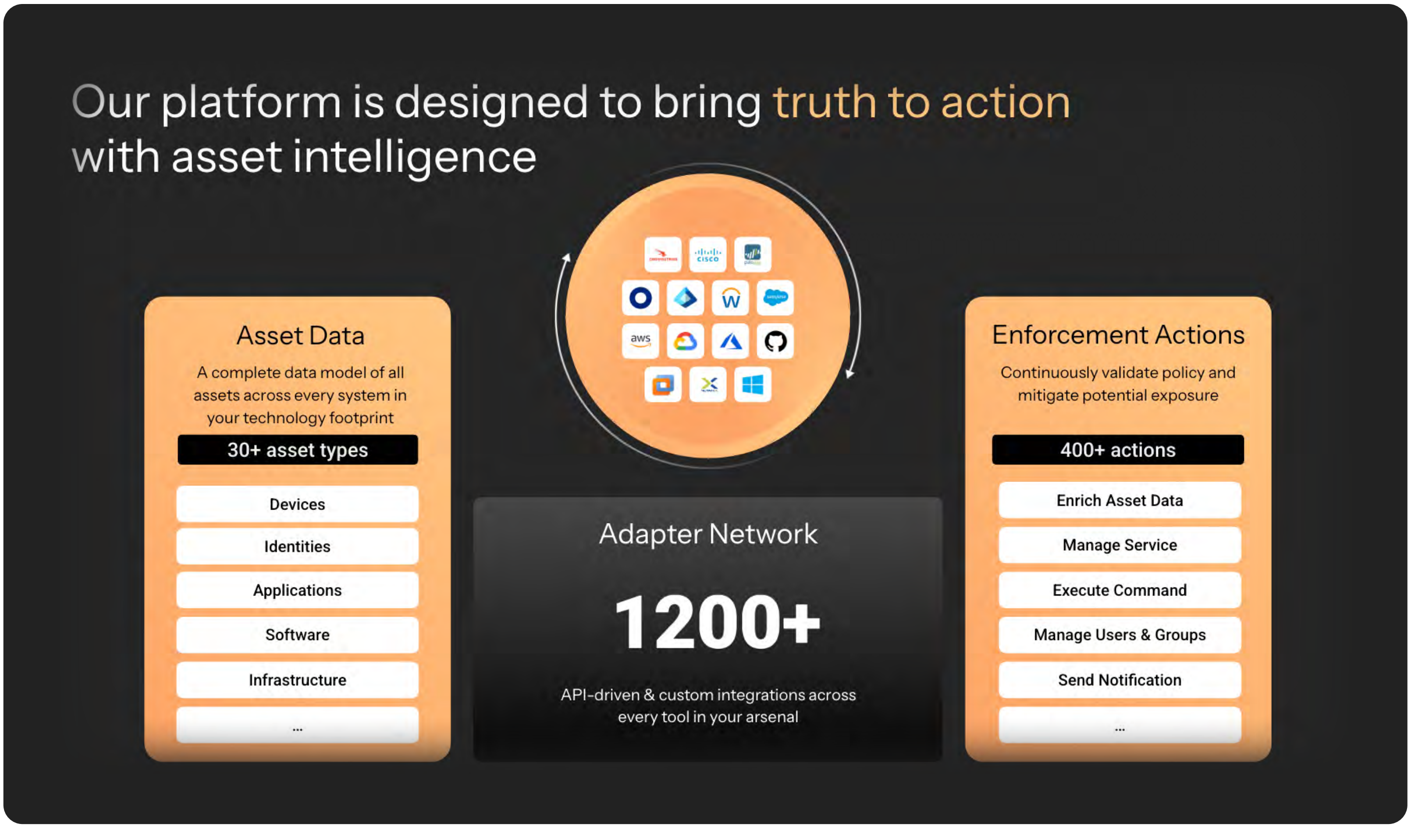
The real challenge today isn't just seeing everything, it's knowing what to do next and why. Exposures, misconfigurations, and inefficiencies inevitably happen every day because everything is so distributed. That's where we come in.

Axonius helps you get a grip on all the assets across your entire technology footprint, and then we turn that intelligence into meaningful action.

Forget the static inventories, disjointed tools, and endless guesswork – we pull asset data from all of your systems – devices, applications, identities, cloud, infrastructure, you name it – into a comprehensive platform.

Our extensive catalog of Adapters, integrates bi-directionally with all of your systems and applications. Once connected, we run an extensive correlation and enrichment pipeline to ensure all asset data is complete, accurate, and always up-to-date. The data model provides total visibility across your attack surface, but we don't stop there – clean asset data unlocks laser sharp actionability that has been impossible to fully realize before due to siloed systems.

The result? Coverage gaps, critical vulnerabilities, risky misconfigurations, excessive spending, and data blind spots are illuminated and optimized before they become issues.



Our platform is designed to bring truth to action with asset intelligence

Asset Data

A complete data model of all assets across every system in your technology footprint

30+ asset types

- Devices
- Identities
- Applications
- Software
- Infrastructure
- ...

Adapter Network

1200+

API-driven & custom integrations across every tool in your arsenal

Enforcement Actions

Continuously validate policy and mitigate potential exposure

400+ actions

- Enrich Asset Data
- Manage Service
- Execute Command
- Manage Users & Groups
- Send Notification
- ...

Axonius transforms asset intelligence into intelligent action.

Preemptively tackle hard-to-spot threat exposures, misconfigurations, and inefficiencies across your entire technology footprint – all in one place backed by one asset data model.

The actionability era of cybersecurity is here – time to bring truth to action with Axonius.

Learn more at www.axonius.com.

Axonius