Axonius

White Paper

ENHANCING CAASM

A More Complete Approach to Cybersecurity Asset Management

Axonius created the term Cybersecurity Asset Management (CAM) years ago to describe a revolutionary approach to understanding assets and their security coverage. Gartner later coined Cyber Asset Attack Surface Management (CAASM), which gained rapid industry adoption as a critical cybersecurity practice.

Gartner's 2024 report, "Emerging Tech: Evolving CAASM Beyond Cyber Asset Management," recognizes that while CAASM remains fundamentally important, it needs to evolve to include more advanced capabilities. The good news? Axonius CAM has included these expanded capabilities from day one, positioning CAASM as a necessary foundation to our more comprehensive approach.

Why Your CAASM Solution Needs to Evolve

According to Gartner and other experts, CAASM remains crucial for enabling security teams to gain a holistic view of assets and exposures. However, today's security challenges require CAASM solutions to improve their capabilities by focusing on:

- Centralized attack surface visibility and prioritization
- Comprehensive asset discovery (including agent-less assets)
- Automated remediation capabilities
- Proactive threat management features

Gartner advises that CAASM vendors must enhance their offerings to play a more central role in exposure management programs and integrate features like automated security control assessment (ASCA). If your CAASM solution hasn't evolved to include these critical capabilities, you're missing out on essential security coverage.

This white paper examines why comprehensive Cybersecurity Asset Management represents a complete approach to managing your digital infrastructure in today's evolving threat landscape, with CAASM capabilities serving as a vital foundation.

The Birth of CAASM: A Security Origin Story

When CEO Dean Sysman co-founded Axonius, he identified a paradox in cybersecurity: despite sophisticated tools to detect, protect against, and remediate threats, security teams still struggled to answer basic questions such as:

- How many Windows devices exist in my environment?
- Are all my virtual machines being scanned properly?
- Which cloud workloads have dangerous misconfigurations?
- Are my security agents actually working?
- Do users have appropriate permissions, or could Bob from accounting accidentally access nuclear launch codes?

Once upon a time, answering these questions might have been simple. Organizations had Windows machines on a physical network, managed by Active Directory, protected by antivirus software, with separate solutions for updates.

Then, like tribbles on the starship Enterprise, the complexity multiplied. Different device types emerged: VMs, Macs, Linux systems, and mobile devices. Organizations implemented disparate solutions to manage and secure these various assets. With cloud migration, new security and management challenges appeared. Now, in the Internet of Things (IoT) era, virtually everything connects to your network, from smart coffee machines to internet-connected fish tanks (yes, those have been breach vectors).

This explosion in device diversity, coupled with the proliferation of security tools, made answering simple inventory questions nearly impossible. It's like trying to count sheep while they're multiplying, changing colors, and occasionally disappearing into another dimension.

The good news? All the necessary data exists. If a solution can collect, deduplicate, normalize, and correlate information from hundreds of different sources, it can:

- Provide a comprehensive, always up-to-date asset inventory
- Uncover security and management gaps
- Automate response actions when assets or users deviate from policies

Cybersecurity Asset Management and the Emergence of Actionability

When categorizing a more capable solution, Axonius discovered we were building something fundamentally different. We couldn't simply piggyback on existing categories, like trying to fit an octopus into a category called "fish with legs."

We created a new category that:

- Clearly described the problems it solved
- Built upon familiar concepts while suggesting innovation
- Signaled a fresh approach to an age-old problem

We called it Cybersecurity Asset Management (CAM), but this term needed clarification:

01 **Definition challenges**
What exactly is an asset? Is it just devices? Users too? Cloud instances? Anything with an IP address?

02 **Terminology conflicts**
"Asset" already had definitions in finance, espionage, and maritime operations.

03 **Historical baggage**
Many IT professionals associate "asset management" with complex spreadsheets or outdated CMDBs full of conflicting, duplicative information.

04 **Ownership disputes**
Security teams point to IT, IT points to desktop support, who points back to security, a pass the buck cycle for accountability.

CAM proved useful precisely because it described a universal problem while highlighting the need for a unified approach, one that transcended traditional departmental boundaries and outdated tools.

The CAASM Hype Cycle: From Buzz to Reality

Gartner's Hype Cycle tracks technology maturity through five phases: Technology Trigger, Peak of Inflated Expectations, Trough of Disillusionment, Slope of Enlightenment, and Plateau of Productivity. It's like a rollercoaster ride for technology adoption, complete with the initial excitement, subsequent nausea, and eventual satisfaction.

Gartner originally defined CAASM as "an emerging technology focused on enabling security teams to solve persistent asset visibility and vulnerability challenges." CAASM strengthens core security functions including:

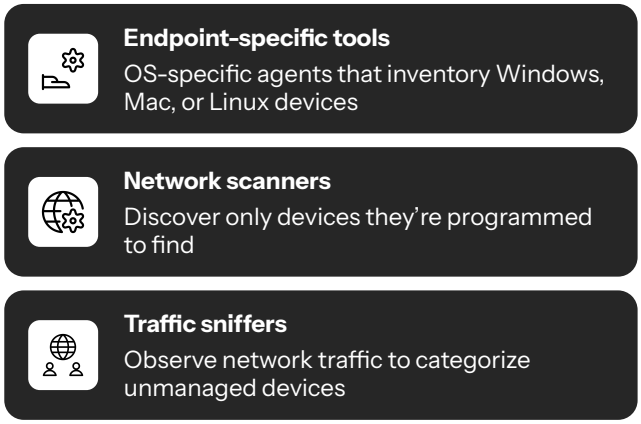
Both CAASM and CAM address asset visibility and security management by:

1. Connecting to existing tools through API integrations
2. Normalizing and correlating data to create a comprehensive inventory
3. Providing queries to identify policy deviations
4. Enabling automated responses based on conditions
5. Offering dashboards to track progress toward security goals

Think of CAASM and CAM as synonyms, but with Axonius, we address and go beyond the essential capabilities Gartner now says are crucial for modern security programs, The Axonius Asset Cloud offers a more comprehensive CAASM approach that includes proactive security measures through enforcements, workflow capabilities, and case management, as well as Actionability with automated remediation and continuous policy enforcement.

Why Traditional Asset Management Falls Short (and Makes Security Teams Nervous)

Many legacy approaches to asset management, including some basic CAASM solutions, focus on limited asset subsets, creating fragmented data and tool management:



These tools provide visibility into asset subsets but come with significant blind spots. It's like trying to map a city by only looking at the roads, or only the buildings, or only the parks. You never get the complete picture.

Fortunately, all this data exists, it's just trapped in separate silos with APIs waiting to be leveraged. This is where the Axonius Asset Cloud with Actionability takes CAASM to the next level.

Five Reasons Organizations Embrace *Axonius Asset Cloud* with Actionability

Axonius customers consistently cite these five primary benefits driving Asset Cloud adoption:

01 **Comprehensive Visibility**: No More Asset Hide-and-Seek

By connecting to 1200+ security and management solutions, Axonius delivers a single system of record for all infrastructure. This means no longer playing detective with your own network or maintaining spreadsheets so large they cause Excel to have an existential crisis.

Without Actionability and more advanced CASSM capabilities, teams are stuck with three inadequate options:

- **Excel**
  Exporting CSVs from multiple sources into monster spreadsheets with more pivot tables than actual data
- **Homegrown scripts**
  Creating, updating, and maintaining scripts that inevitably break during critical security incidents
- **CMDB**
  Relying on a system that's perpetually outdated the moment it's populated

02 **Unified Query Capabilities**: Ask Once, Get Answers Everywhere

Axonius allows security teams to ask questions spanning all data sources, from basic inventory ("How many Windows devices do I have?") to complex security queries ("Which Windows 10 devices running vulnerable Chrome versions have non-functioning EDR agents?").

03 **Automated Compliance:** From Audit Panic to Audit Peace

With comprehensive asset inventory and policy adherence queries, organizations can save weeks of manual work by automating audit responses and regulatory compliance reporting. Imagine being able to simply press a "make auditors happy" button.

04 **Unified Source of Truth:** Ending IT vs. Security Battles

When IT and security teams operate from different data sources, they inhabit parallel universes. Axonius integrates data from multiple sources into a single view, ensuring everyone makes decisions based on the same information.

04 **Future-Proofed Security Stack:** Change Tools Without Breaking Everything

The only constant in security is change. New tools arrive, old tools disappear, vendors are acquired. A comprehensive Actionability solution lets you add, remove, or replace tools while maintaining consistent visibility, query capabilities, and automated responses.

Real-World *Use Cases*

Incident Response: When Minutes Matter

When investigating incidents, SOC teams need immediate access to comprehensive asset information. With Axonius, security analysts can accelerate investigations by answering critical questions:

- Which devices and users were involved in the alert?
- Where are the devices located?
- What software runs on affected assets?
- Which users have access to compromised systems?

Axonius provides a RESTful API to push data to SIEM and SOAR platforms, enabling focused investigations from a single console.

Vulnerability Management: Finding the Needles in Your Digital Haystack

Axonius solves two major vulnerability challenges:

1. Identifying unscanned assets: Finding devices or cloud instances not being assessed
2. Prioritizing by CVE: Quickly locating vulnerable assets when new threats emerge

Endpoint Management: Ensuring Your Digital Army Has Armor

Common endpoint challenges solved by Axonius include:

- Finding devices missing security agents
- Identifying installed-but-not-functioning agents
- Ensuring agents run the latest versions

The problem isn't knowing which devices have agents (any console can tell you that), it's knowing which devices should have agents but don't. It's also understanding context: if your security policy requires different agents for different platforms, how do you ensure the right agent is deployed to the right device?

CMDB Reconciliation: Ensuring Your Single Source of Truth is Accurate

CMDBs often fail as reliable asset inventories, especially with ephemeral cloud resources. Data conflicts due to inconsistent naming conventions and field formats make matters worse.

Axonius aggregates and deconflicts asset data to provide a singular, credible view into any asset, answering questions like:

- How many assets are missing from the CMDB?
- Which "disposed" devices in the CMDB are still active?
- Do CMDB device details match current reality?

Proving the Business Value: Because "Trust Me" isn't a Business Case

Security solutions typically struggle to demonstrate ROI, how do you measure the value of breaches that didn't happen?

Actionability solutions like Axonius uniquely show objective business value by:

1. Calculating the hours saved through automation
2. Demonstrating the full value of existing security investments
3. Quantifying risk reduction through security gap identification

Choosing the Right Solution: *Six Critical Questions*

When evaluating any CAASM solution, you should ask these six questions:

01

Can it uncover security gaps you didn't know existed?

Complexity creates blind spots, which create security incidents. A comprehensive CAASM solution should provide complete visibility to reveal hidden gaps.

02

Can it continuously inventory your entire attack surface?

Manual inventories are tedious, error-prone, and immediately outdated. Effective Actionability solutions discover all assets, physical, virtual, and ephemeral, across on-premise and cloud environments.

03

Does it require custom integration work?

Security teams can't wait for vendors to build custom integrations. The best solutions have pre-built adapters ready to deploy.

04

Can it automate policy enforcement and remediation?

Finding gaps is only half the battle, you need automation to close them efficiently. Look for pre-built automations and open APIs.

05

How extensive is its integration ecosystem?

Technology stacks constantly evolve. Verify that a CAASM provider supports not just your current tools but potential future additions.

06

Does it normalize and correlate data effectively?

Anyone can fetch API data, but creating a unified view requires sophisticated normalization and correlation. Test this thoroughly during evaluations.

The Axonius Advantage: Not Just Another CAASM Solution

Axonius delivers a true Actionability platform that addresses all modern and pervasive requirements, building on CAASM's critical foundation while providing the enhanced capabilities Gartner now recommends.

Comprehensive Visibility Without the Hassle

The Axonius Asset Cloud connects to 1200+ sources of business, IT, and security data, without requiring agents, to inventory all assets in hours, not days or weeks. This eliminates blind spots and provides the foundation for effective cybersecurity.

Uncovering Unknown Unknowns

Our platform continually surfaces coverage gaps, detecting and accounting for changes in assets, configurations, and controls. You'll gain visibility into all assets, allowing you to close security gaps before they become incidents.

Complete Asset Inventory Without the Heavy Lifting

Axonius inventories all devices, cloud services, software applications, and users, regardless of location or power state, by leveraging your existing tools and data. No agents to install, no network scanning required.

Seamless Integration with Your Existing Stack

With integrations to hundreds of sources, Axonius delivers unmatched flexibility. Switch security providers seamlessly, monitor new deployments, and identify legacy software, all while maintaining complete visibility.

Automated Policy Enforcement When It Matters Most

Any query within Axonius can trigger automated actions when assets or users deviate from policies. Alert teams, create contextualized tickets, expand vulnerability scans, update CMDBs, or manage user accounts, all without manual intervention.

Battle-Tested Correlation Engine

Having built hundreds of integrations for hundreds of customers, Axonius has encountered more data sources, edge cases, and correlation challenges than virtually any competitor. Our dedicated team continuously refines our correlation logic, making it more accurate every day.

Conclusion: Extending CAASM with Actionability

As Gartner now recognizes, while CAASM provides essential capabilities for security teams, it needs to evolve to include more advanced features. The Axonius Asset Cloud has always incorporated these enhanced capabilities that Gartner now recommends, positioning CAASM as a necessary foundation within our more comprehensive approach.

Axonius gives security leaders the confidence to control complexity by mitigating threats, navigating risk, automating responses, and informing business strategies. With solutions that exceed all requirements for CAASM and SaaS management, the Axonius Asset Cloud deploys in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically enforce policies.

Cited as one of the fastest-growing cybersecurity companies, with accolades from CNBC, Forbes, and Fortune, Axonius covers millions of assets for customers worldwide.

See how the Axonius Asset Cloud with Actionability correlates asset data from your existing solutions to provide an always up-to-date inventory, uncover gaps, and automate action.
For more information and a platform demo, visit Axonius.com

Request a Demo

Axonius