Axonius

Axonius Cyber-Physical Assets

Unifying Visibility and Actionability across IT, IoT, and OT

Modern enterprises operate across a hybrid physical-digital landscape where IT systems, IoT devices, OT infrastructure, and cyber-physical assets are deeply interconnected. From manufacturing floors and utilities to healthcare networks and smart facilities, these environments are critical to business continuity, yet largely invisible to traditional security tools.

Axonius CPA changes that.

Axonius Cyber-Physical Assets (CPA) extends the Axonius Platform beyond traditional IT, delivering unified visibility, contextual risk insight, and safe actionability across cyber-physical environments, at scale and without disruption.

Using passive discovery, deep device intelligence, and policy-driven workflows, Axonius CPA helps security, IT, OT, and operations teams understand what's connected, why it matters, and how to reduce risk without impacting critical systems.

Why Axonius CPA

See Every Asset. Understand Every Risk. Act With Confidence.

Axonius CPA brings cyber-physical assets into the Axonius Platform, unifying IT, IoT, and OT visibility with contextual risk intelligence and automated, safe response.

The result is one platform that helps organizations:

- Discover unmanaged and agentless devices
- Understand risk in operational context
- Reduce exposure without disrupting critical systems

What Axonius CPA *Delivers*

1 Unified Visibility Across Cyber-Physical Environments

See and understand every connected asset across IT, IoT, and OT from a single source of truth. Passive network discovery combined with selective active identification and 1,300+ Axonius integrations aggregates, normalizes, and correlates asset data across endpoints, infrastructure, and cyber-physical devices.

2 Context That Goes Beyond CVEs

Prioritize risk based on real-world impact, not just vulnerability scores. Deep device fingerprinting (150+ attributes), behavioral insights, and enriched context factor in device role, exploitability, communication behavior, and operational impact, not just CVSS.

3 Actionability Without Disruption

Reduce risk safely in environments where downtime isn't an option. Policy-driven workflows, tagging, segmentation planning, and integrations with NAC, firewalls, and ITSM, without agents, scans, or operational disruption.

4 Continuous Compliance Across IT and OT

Move from point-in-time audits to continuous control validation. Built-in dashboards and reporting aligned to frameworks such as HIPAA, NIS2, IEC 62443, and HICP help organizations maintain awareness of cyber-physical security posture and compliance across operational environments.

5 Consolidation With Purpose

Extend your Axonius investment into cyber-physical environments, without adding another silo. CPA operates as a native extension of Axonius Cyber Assets and Exposures, expanding coverage while reducing tool sprawl.

Benefits at a Glance - Managing What *You Couldn't See Before*

1 Always Know What's Connected - Without Disruption

Eliminate blind spots across IoT, OT, and cyber-physical environments. Establish a trusted, continuously updated system of record for every connected device, even those that can't run agents or be safely scanned. Axonius CPA passively discovers, identifies, and classifies cyber-physical assets, enabling teams to see what exists, who owns it, and the risk associated.

2 Prioritize the Risks That Actually Matter

Focus on real-world exposure, not theoretical vulnerability scores. Understand which cyber-physical risks could actually disrupt operations. Axonius CPA contextualizes device risk based on behavior, configuration, communication patterns, and exposure, helping teams identify weak credentials, outdated firmware, unsafe protocols, and insecure segmentation without putting systems at risk.

3 See the Full Blast Radius Before Incidents Escalate

Understand how physical systems amplify digital risk. Connect cyber-physical assets to applications, identities, networks, and vulnerabilities in one unified asset graph. By feeding CPA data into Axonius CA and Exposures, teams can assess impact faster, prioritize remediation smarter, and respond to incidents with confidence, not guesswork.

4 Reduce Lateral Movement Without Breaking Critical Systems

Validate segmentation safely before enforcing change. Lower the risk of outages while strengthening security. Axonius CPA analyzes real communication patterns so teams can validate segmentation assumptions, model policy changes, and eliminate unnecessary trust relationships, before enforcement ever happens.

5 Stay Audit-Ready Without the Fire Drills

Move from point-in-time compliance to continuous validation. Maintain continuous evidence of cyber-physical controls across regulated environments. Axonius CPA automatically validates inventory completeness, segmentation coverage, vulnerability posture, and control drift, replacing spreadsheets and manual audits with always-on visibility.

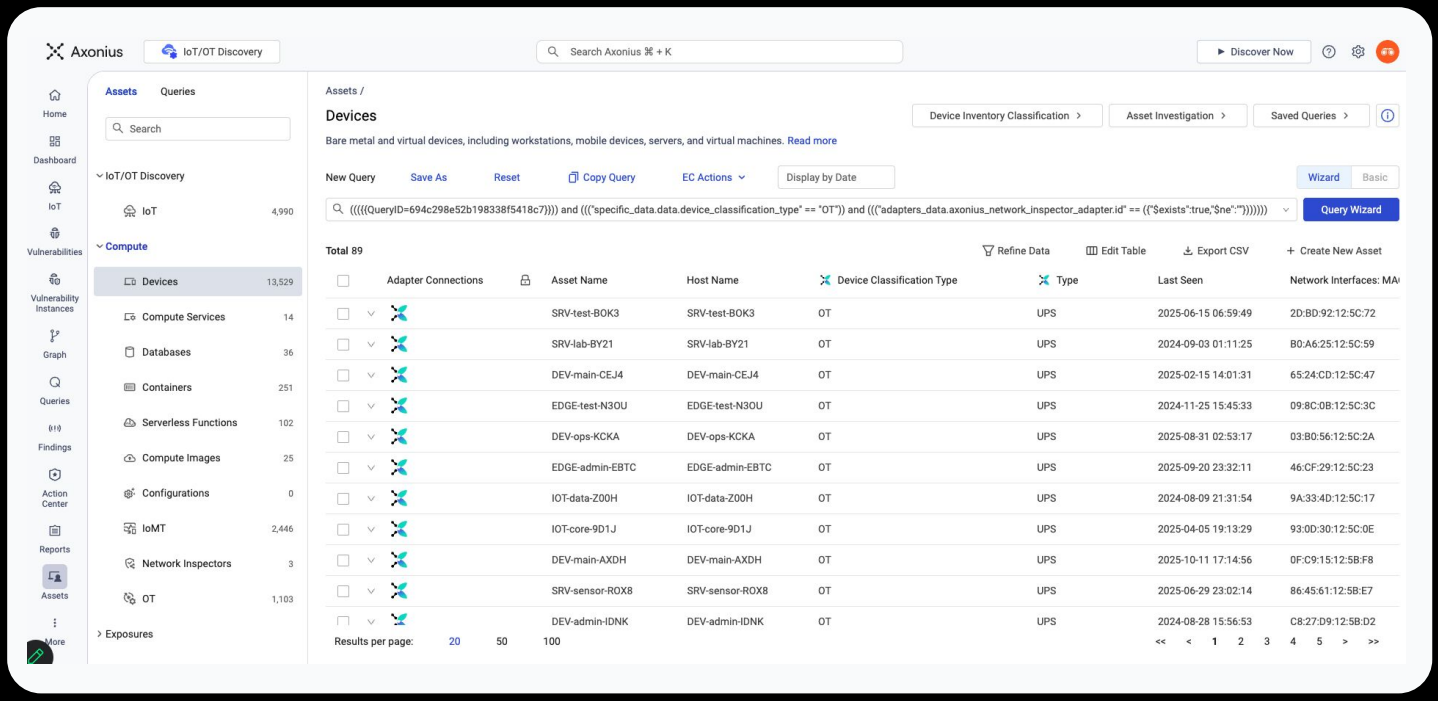
6 Simplify the Stack While Expanding Coverage

Extend your existing Axonius investment into cyber-physical environments. Reduce tool sprawl without sacrificing insight. Axonius CPA expands the Axonius Asset Cloud into IoT and OT environments, allowing teams to consolidate overlapping point tools and manage cyber-physical risk through the same workflows they already trust.

Completing the Asset Story: *CAM + CPA Together*

Capability	Axonius Cyber Assets (CAM)	Axonius Cyber-Physical Assets (CPA)	Business Benefit
Asset discovery	Discovers IT assets from 1,300+ integrations	Passively discovers IoT, OT, and cyber-physical devices from the network	Full asset visibility without blind spots
Agentless visibility	Yes (via integrations)	Yes (via passive network inspection)	Safe discovery in sensitive environments
Device classification	IT endpoints, servers, cloud, network	PLCs, sensors, cameras, building systems, medical & industrial devices	Accurate inventory across digital + physical
Asset normalization	Deduplicates and correlates IT assets	Correlates cyber-physical assets into the same asset graph	One trusted system of record
Ownership & context	IT ownership, business units, tags	Adds site, facility, network zone, operational role	Faster remediation and accountability
Vulnerability context	CVEs and misconfigurations for IT assets	Firmware, protocol, exposure, and segmentation context for physical devices	Risk prioritized by real-world impact
Network visibility	Limited (tool-reported)	Native visibility into device communications	Understand “who talks to what”
Exposure analysis (with Exposures)	IT-focused exposure paths	Extends exposure analysis to IoT/OT assets	Accurate blast radius analysis
Enforcement workflows	Tags, tickets, integrations	Extends the same workflows to cyber-physical assets	Action without disruption
Compliance support	IT-centric evidence	Continuous validation across IT + OT controls	Audit readiness without manual effort

One Platform.
Every Asset.



Bring Cyber-Physical Assets
Into the Platform You Already Trust.

Visit www.axonius.com

Learn more

Axonius