



# Cybersecurity Asset Management Platform

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security coverage gaps, and automatically validates and enforces your security policies.

By seamlessly integrating with roughly 400 security and IT management solutions (and counting), Axonius deploys in hours, not weeks, to improve IT and security operations, including incident response, vulnerability and patch management, configuration management, and more.

**AXONIUS**

Discover Now

Devices

New Query [Unsaved] Save As Reset Display by Date

Q ((adapters\_data.aws\_adapter.public\_ips == (('exists':true,'\$ne':''))) and not ((adapters\_data.epo\_adapter.id == (('exists':true,'\$ne':''))) and not ((adapters\_data.tenable\_security\_center\_adapter.id == (('exists':true,'\$ne':'')))))

Saved Queries Query Wizard

Devices (67)

	Adapter Connections	Asset Name	Host Name	Last Seen	Network Interfaces:
<input type="checkbox"/>	<input checked="" type="checkbox"/>	labapache-17686-beta		2020-05-20 23:01:21	88.53.2E.12.9F:A6
<input type="checkbox"/>	<input checked="" type="checkbox"/>	db17936-beta		2020-05-20 19:09:43	88.53.2E.12.A0:A0
<input type="checkbox"/>	<input checked="" type="checkbox"/>	externalmongo-18049-prod		2020-05-19 01:37:13	88.53.2E.12.A1:11
<input type="checkbox"/>	<input checked="" type="checkbox"/>	infralb-18428-prod		2020-05-19 13:37:05	88.53.2E.12.A2:8C
<input type="checkbox"/>	<input checked="" type="checkbox"/>	externalnginx-18495-prod		2020-05-19 01:57:28	88.53.2E.12.A2:CF
<input type="checkbox"/>	<input checked="" type="checkbox"/>	web18725-dev		2020-05-19 15:15:19	88.53.2E.12.A3:B5
<input type="checkbox"/>	<input checked="" type="checkbox"/>	infra18797-prod		2020-05-21 04:59:40	88.53.2E.12.A3:FD
<input type="checkbox"/>	<input checked="" type="checkbox"/>	labapache-19019-beta		2020-05-19 15:36:06	88.53.2E.12.A4:DB
<input type="checkbox"/>	<input checked="" type="checkbox"/>	labnginx-19400-stg		2020-05-20 20:21:41	88.53.2E.12.A6:58
<input type="checkbox"/>	<input checked="" type="checkbox"/>	websql-19987-stg		2020-05-20 13:03:07	88.53.2E.12.A8:A3
<input type="checkbox"/>	<input checked="" type="checkbox"/>	infrasql-20008-prd		2020-05-19 04:38:26	88.53.2E.12.A8:B8
<input type="checkbox"/>	<input checked="" type="checkbox"/>	lab20451-prod		2020-05-18 13:32:28	88.53.2E.12.AA:73
<input type="checkbox"/>	<input checked="" type="checkbox"/>	dbsql-20497-prd		2020-05-19 19:37:44	88.53.2E.12.AA:A1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	dbnginx-20568-stg		2020-05-20 13:58:58	88.53.2E.12.AA:E8
<input type="checkbox"/>	<input checked="" type="checkbox"/>	monitornginx-20726-beta		2020-05-20 23:50:20	88.53.2E.12.AB:86
<input type="checkbox"/>	<input checked="" type="checkbox"/>	monitor20769-dev		2020-05-20 12:42:04	88.53.2E.12.AB:B1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	db20797-beta		2020-05-21 00:48:59	88.53.2E.12.AB:CD
<input type="checkbox"/>	<input checked="" type="checkbox"/>	webmongo-20801-prd		2020-05-19 16:58:06	88.53.2E.12.AB:D1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	dbsql-20815-stg		2020-05-19 19:39:06	88.53.2E.12.AB:DF
<input type="checkbox"/>	<input checked="" type="checkbox"/>	monitormongo-21292-prd		2020-05-20 21:54:06	88.53.2E.12.AD:BC

Enforcement Center • New Enforcement Set

Enforcement Set Name

Main Action...

Success Actions ...

Failure Actions ...

Post Actions ...

Trigger

Enforcement Name is a required field

Save & Run Save & Exit

RESULTS PER PAGE: 20 50 100

1 2 3 4

Action Library

Notify

Create Incident

Axonius Utilities

Enrich Device or User Data

Update VA Coverage

Run Command

Execute Endpoint Security Agent Action

Isolate in Carbon Black CB Response

Unisolate in Carbon Black CB Response

Isolate in Cyberason Deep Detect & Respond

Unisolate in Cyberason Deep Detect & Respond

Change Carbon Black CB Defense Policy

Isolate Carbon Black CB Defense Device

Unisolate Carbon Black CB Defense Device

Initiate SentinelOne Scan

Automox Install Update

Create CMDB Computer

SEAMLESS INTEGRATION

## COMPREHENSIVE ASSET INVENTORY



“As the saying goes, you can’t manage what you can’t see. If you don’t know what you have on the network, you’re not managing it - and it’s almost surely vulnerable. This tool gives us clear visibility into compliance across our systems, so we can make sure our assets are properly managed, fully accounted for, and the like.”

— STEVE KJAER  
CISO, POLY

## How it works.

### CHOOSE YOUR DEPLOYMENT OPTION

Deploy Axonius on-premise or private cloud, or as an AWS-hosted SaaS solution. Axonius is an **agentless solution** and doesn’t need to scan your networks - instead we discover assets using adapters.

### CONNECT ADAPTERS

Connect to the different solutions you already use with Adapters - pre-built integrations on the Axonius platform.

### EXAMINE YOUR ASSETS AND TAKE ACTION

Axonius provides a fully unique list of devices, users, and cloud assets in your environment, so you can surface areas of risk and be alerted when policies aren’t met.

## Key Benefits

### REDUCE MEAN TIME TO IT ASSET INVENTORY

Axonius correlates data from all sources to provide a continuous, up-to-date inventory of all unique assets.

### DISCOVER COVERAGE GAPS AND SURFACE RISK

Understand when assets are missing critical security controls and when they have unsanctioned or vulnerable software.

### VALIDATE POLICIES AND AUTOMATE RESPONSE

Whenever assets deviate from policies or desired states, the Axonius Security Policy Enforcement Center is used to notify personnel, enrich data, or configure assets automatically.

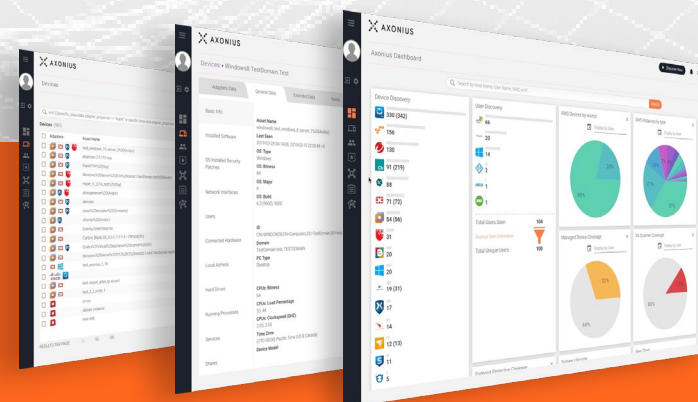
## Use Cases

### FOR IT PROFESSIONALS

- **Device Discovery**
  - Unmanaged vs. Managed Devices
  - Ephemeral Devices
- **Endpoint Management**
  - Devices Missing Agents
  - Devices with Agents Not Functioning
- **Configuration Management**
  - CMDB Reconciliation
  - Configuration Monitoring

### FOR SECURITY PROFESSIONALS

- **Security Control Validation**
  - Find devices with missing or malfunctioning security controls
  - Find exploitable devices missing vulnerability scans and patches
  - Identify rogue devices and unwanted software
- **Incident Response**
  - Understanding Device Coverage and Context
  - Pivoting Between Alert Device State and Users
- **Vulnerability Management**
  - Devices Not Being Scanned
  - Prioritizing CVEs
- **GRC Audit**
  - Meeting Benchmarks and Regulations
  - Satisfying Audit Requirements
- **Security Policy Enforcement**
  - Notify the right teams when assets don’t meet policies
  - Enrich device and user data with third party contextual data sources (i.e. Shodan, Censys, HavelBeenPwned)
  - Remediate machines via endpoint security agents or direct commands



Axonius is the cybersecurity asset management platform that lets IT and Security teams see devices for what they are in order to manage and secure all. **Interested in seeing what Axonius can do for your organization?**

LET’S TALK →