

CYBERSECURITY ASSET

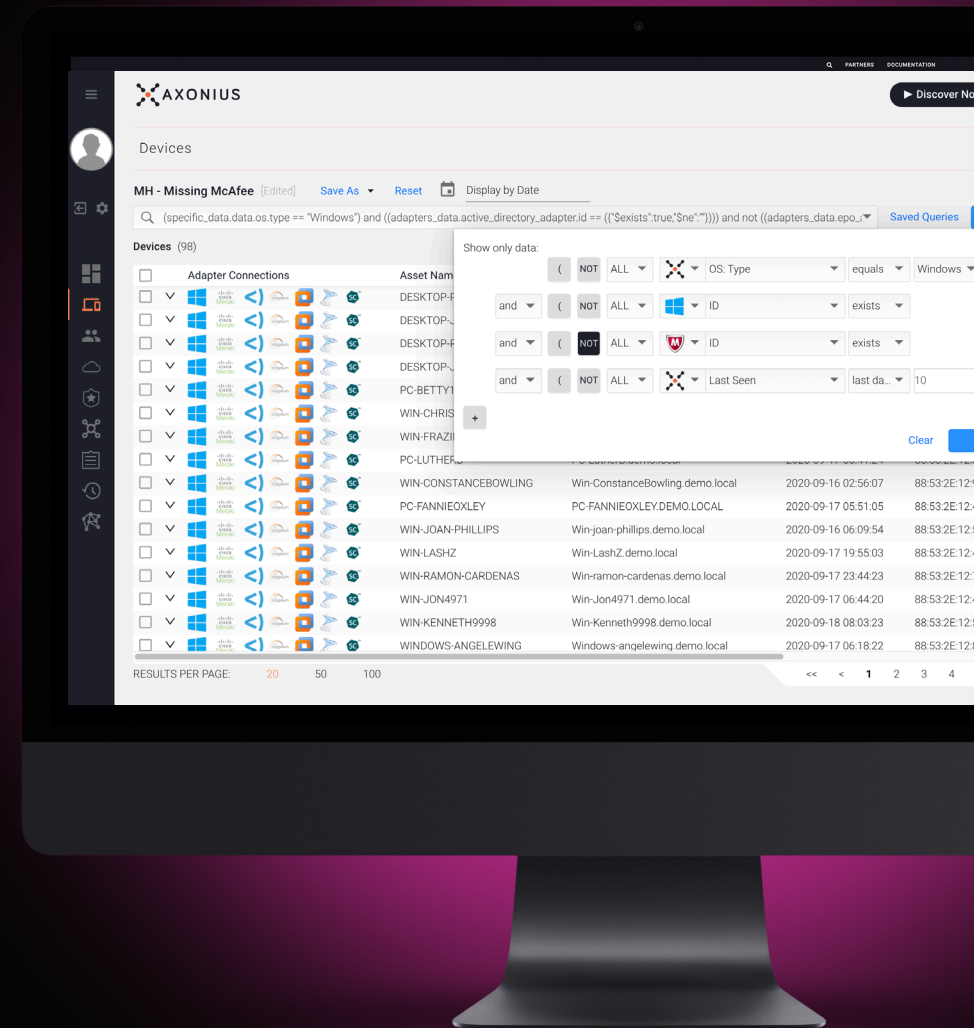
MANAGEMENT PLATFORM



AXONIUS

Axonius is the cybersecurity asset management platform that **gives organizations a comprehensive asset inventory, discovers security coverage gaps and identifies risk, and automatically validates your security policies.**

By seamlessly integrating with over 600 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.



KEY BENEFITS

REDUCE MEAN TIME TO 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 I.T. 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

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

- Understand device coverage and context
- Pivot between alert device state and users

Vulnerability Audit

- Meet benchmarks and regulations
- Satisfying audit requirements

Vulnerability Management

- Identify known vulnerabilities across the environment
- Prioritize CVEs
- Contextualize vulnerabilities with device data

Security Policy Enforcement

- Notify the right team when assets don't meet policies
- Enrich device and user data with third party contextual data sources
- Take custom actions with direct commands or the [Axonius API](#)

“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

- 1. CHOOSE YOUR DEPLOYMENT OPTION**
Deploy Axonius as a *customer-hosted*, or as an *Axonius-hosted* solution.
- 2. CONNECT ADAPTERS**
Connect to different solutions you already use with Adapters - pre-built integrations on the Axonius platform.
- 3. 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.



Interested in seeing what Axonius can do for your organization?

axonius.com