

Secure *M&A*, Minus the Headache

Minimize Risk and Accelerate Integration with Axonius

The M&A Challenge:

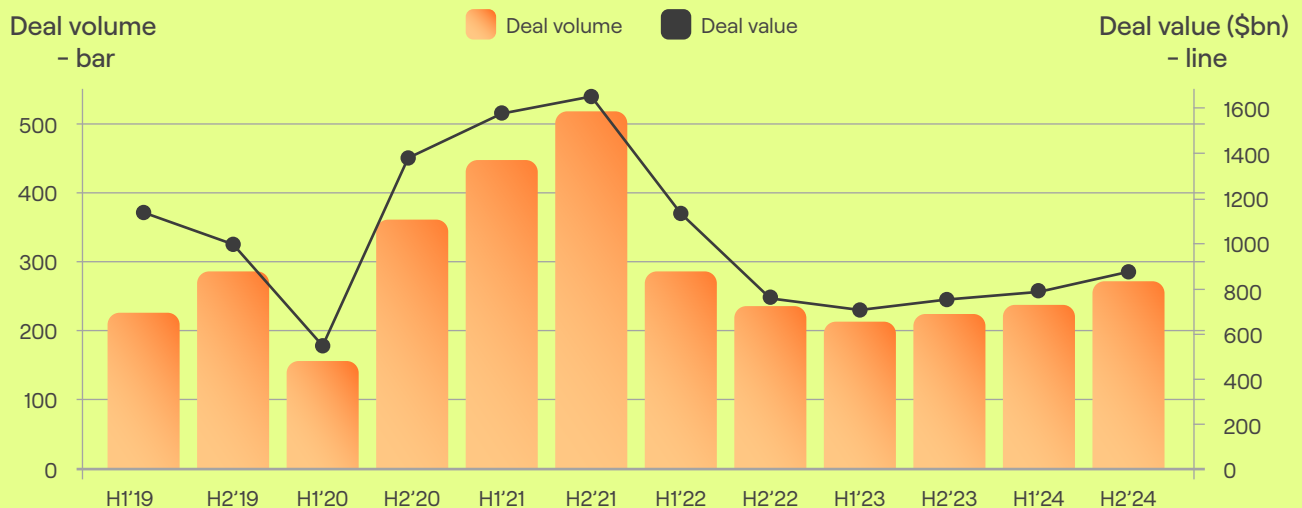
High Stakes, Low Visibility

Since 2020, nearly 56,000 M&A deals have closed each year. In 2024 alone, over 500 acquisitions topped the \$1 billion mark, with 72 megadeals exceeding \$5 billion (PwC). Given these staggering figures, reducing operational risk and accelerating technical integration isn't just desirable, it's mission critical.

Here's the problem: While your organization may get audited financial statements on the other firm to assess fiscal health, you're often flying blind on the actualities of cyber asset hygiene (and really, all IT hygiene) until after the deal closes.

Your IT and Security teams face a sea of unknown assets, conflicting policies, and incomplete or inaccurate data. All of this needs to be resolved quickly to prevent costly downtime, revenue loss, or security breaches.

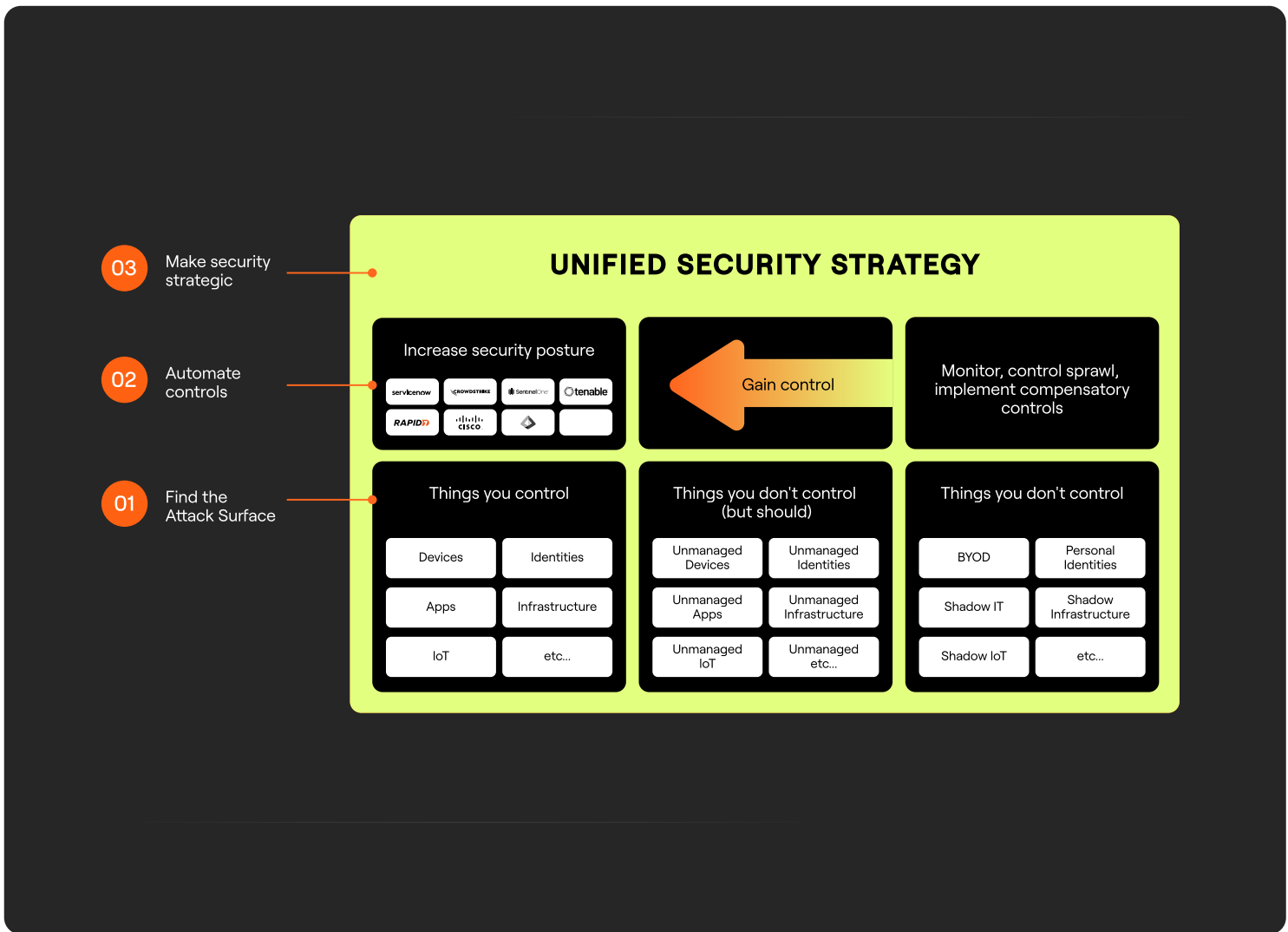
Deals over *\$1bn*, 2019-2024



Enter Axonius:

Your M&A Navigation Guide

Axonius cuts through the fog, delivering crystal-clear visibility into virtually all IT assets, both yours and the acquired company's, to help inform smarter decisions and ensure seamless integration. To follow is your navigation guide for M&A smooth sailing, especially during that critical "don't break anything" phase when the ink is still wet.



1. Discover Everything You Just *Acquired*

Documentation can be deceiving. Even a CMDB can be deceiving. That's the harsh truth about understanding your newly acquired environment. Most companies lack a comprehensive, accurate asset inventory, creating dangerous blind spots for your IT and security teams.

Axonius eliminates these blind spots by connecting to 1,200+ enterprise apps across business, IT, and security data, without installing agents, to inventory all assets in hours, not months. No more unwanted surprises lurking in your new digital harbor. This includes identifying the assets that are both known and unknown (or managed and unmanaged).

Axonius is the system of truth to *secure your cyber assets*

Cyber Assets



Things you control

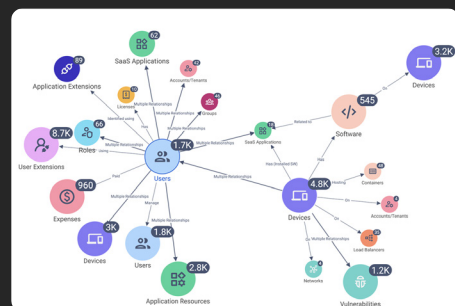
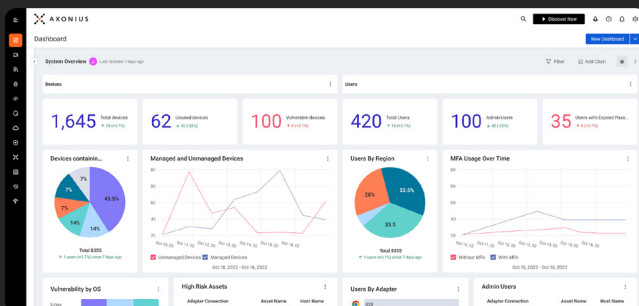


Things you don't control
(but should)



Things you can't control

Attack Surface



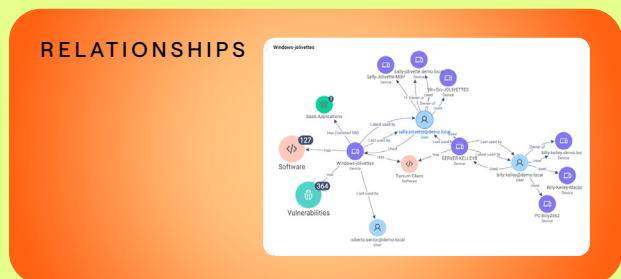
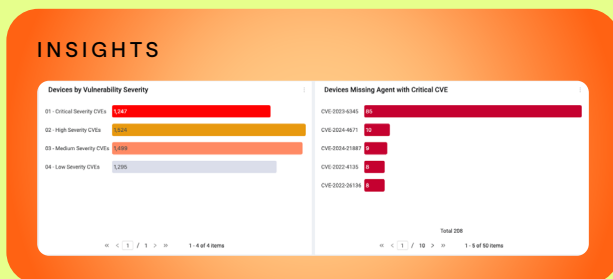
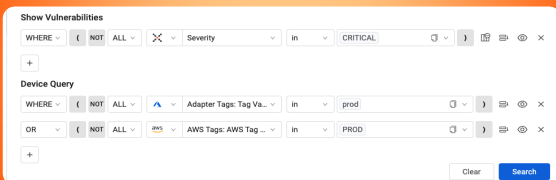
2. Expose the *Real Security* Posture

Let's be honest, every company "dresses up" during due diligence. That "fully protected" environment? It's often far less secure than advertised. Post-acquisition, Axonius eliminates surprises by revealing the naked truth through comprehensive asset and user visibility.

With Axonius, you can instantly:

- Identify system environments ripe for integration
- Pinpoint secure environments worth expanding
- Flag environments or applications that should be retired
- Expose critical risk factors like:
 - Devices missing security agents
 - Unauthorized or end-of-life software
 - Users with excessive privileges
 - Devices skipped by vulnerability scanning

Axonius provide many ways of *getting insights*

QUERIES

Show Vulnerabilities

WHERE: NOT ALL Severity in CRITICAL 1

Device Query

WHERE: NOT ALL Adapter Tags: Tag Va... in prod 1

OR: NOT ALL AWS Tags: AWS Tag ... in PROD 1

Clear Search

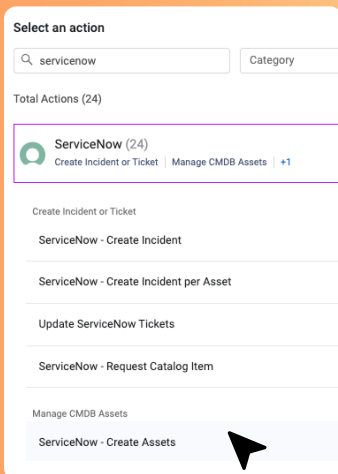
3. Automate, Remediate, Celebrate

Without automation, tracking progress and maintaining momentum becomes an arduous task. Axonius continuously updates reporting as you integrate new assets, showcasing your progress during large-scale integration projects.

The platform doesn't just identify problems, it solves them. Leveraging point-in-time custom enforcement actions and continuous workflows, customers can optimize security policy enforcement across your newly expanded empire.

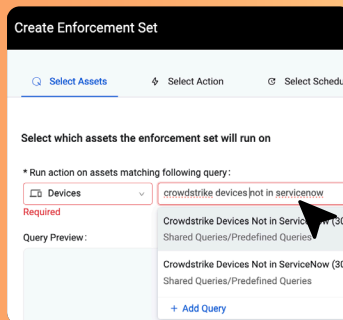
Step 1

Choose the Create Assets action



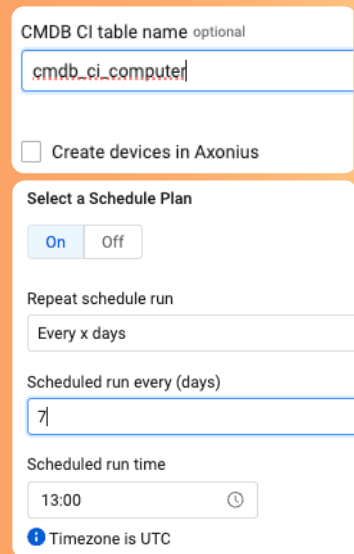
Step 2

Specify your saved query



Step 3

Choose a CMDB table & set an update frequency



The Axonius Edge

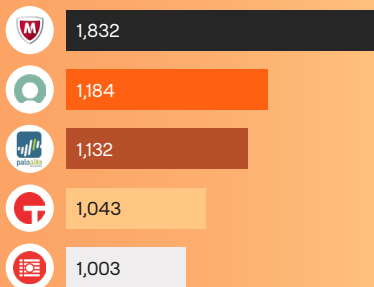
Deploy in Days, Not Weeks

Axonius delivers a true system of record for your entire digital infrastructure, including hardware, software, SaaS apps, cloud services, identities, data systems and more. By connecting to thousands of data sources, the platform offers IT and security teams a comprehensive inventory, uncovers gaps, and triggers automated responses whenever devices and users stray from policies.

Enterprise Asset View

Last Updated 7 months ago

Devices by Data Source

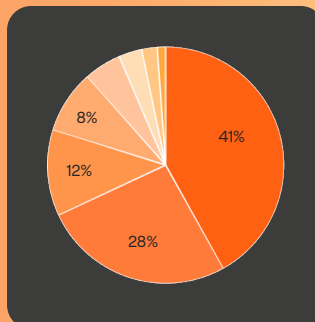


Total 18,701 unique Devices

< 1 / 8 >

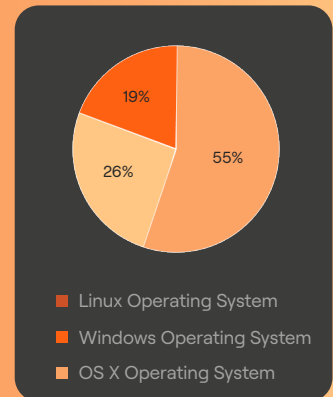
1 - 5 of 39 items

Active Windows Workstations



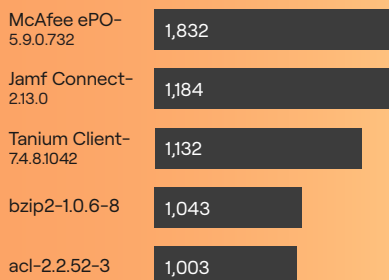
Total 784

OS Breakdown



Total 3,952

Installed Software - All Devices



Windows Servers



Use Axonius to *Reduce M&A Risk*



Instantly Visualize What You've Acquired

No network scans. No endpoint agents. Just connect to solutions you already use and get a complete asset inventory within a few days.



Immediately Spot Exposures

Devices missing security agents, critical vulnerabilities, unscanned public-facing assets, expired user credentials, and more.



Automatically Enforce Organizational Security Policy

When integrated assets violate security policies, the Enforcement Center can take hundreds of actions including notifying teams, enrich device and user data, deploying files and commands to neutralize risks, and even reconciling with your CMDB.

Don't let your next acquisition become your next IT or security shipwreck. With Axonius, you can transform M&A integration into a competitive advantage.

Interested in seeing what Axonius can do for your organization?

[Request a demo](#)