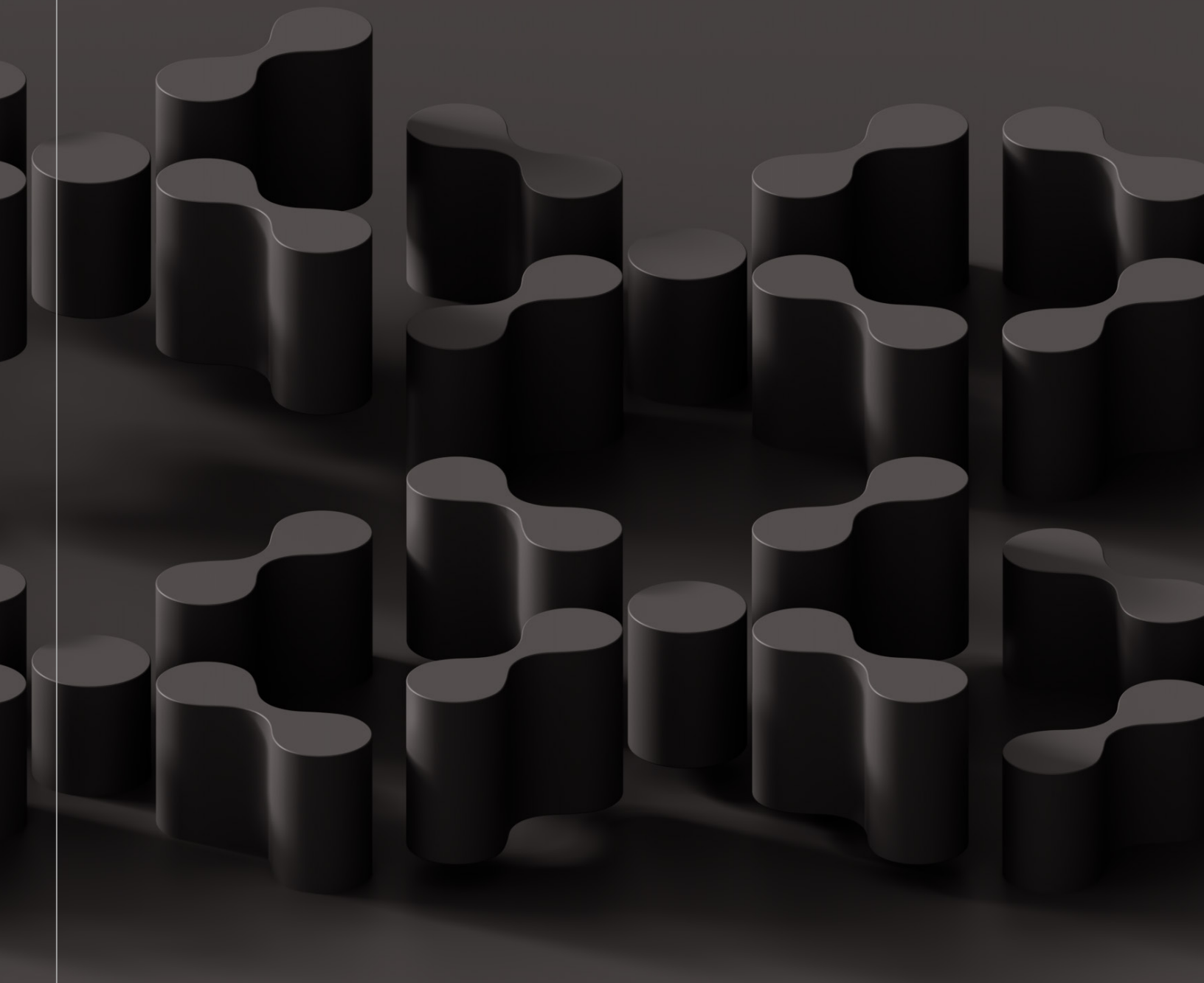
Axonius

Buyer's Guide for Security and IT

Getting buy-in across teams to deploy a modern cyber asset attack surface management solution

March 2025



Intro

You've done your homework, evaluated all your options, and have decided that a new, better approach to discovering, managing, and remediating your cyber assets needs to be prioritized in your technology environment. Now comes the next step: *getting buy-in across teams to purchase a new solution*. Consider this your secret weapon. Read on for a comprehensive guide to pitching a new approach to cyber asset management to other business leaders.

Getting buy-in from *IT teams*

For IT teams, having an accurate asset inventory is a no-brainer. That said, most IT organizations already have a product in place, most commonly a CMDB, to manage their assets. But, you'll likely need input and ongoing support from IT to deploy and manage a cyber asset management solution, even if IT isn't going to be the primary owner. And, of course, it would be great to share the budget, too. The challenge here becomes convincing IT that a cyber asset management solution can complement, rather than replace, their existing CMDB.

The CIO POV

A good CIO is typically security-minded, even if not the primary owner of cybersecurity in the organization. That said, IT teams that have already invested heavily in a CMDB are going to be very hesitant to move to a new solution from both a resource and cost perspective. It's the "why fix something that's not broken?" mentality. As a security leader, your job will be to convince IT about how to complement the CMDB to better address security-focused use cases.

The talk track

- CMDBs were great when the attack surface was more manageable, and are still a great solution to manage IT service management processes. But, the security teams need more
- We need better insight into both known and unknown assets accessing our corporate resources
- With a CAASM, we extend the capabilities of a CMDB by providing the security insights required to support scenarios like incident response, security posture management, and more - we can even integrate with ServiceNow for more streamlined ticket management

Teams in the CIO (IT) org

- IT Procurement
- Digital Innovation and Strategy

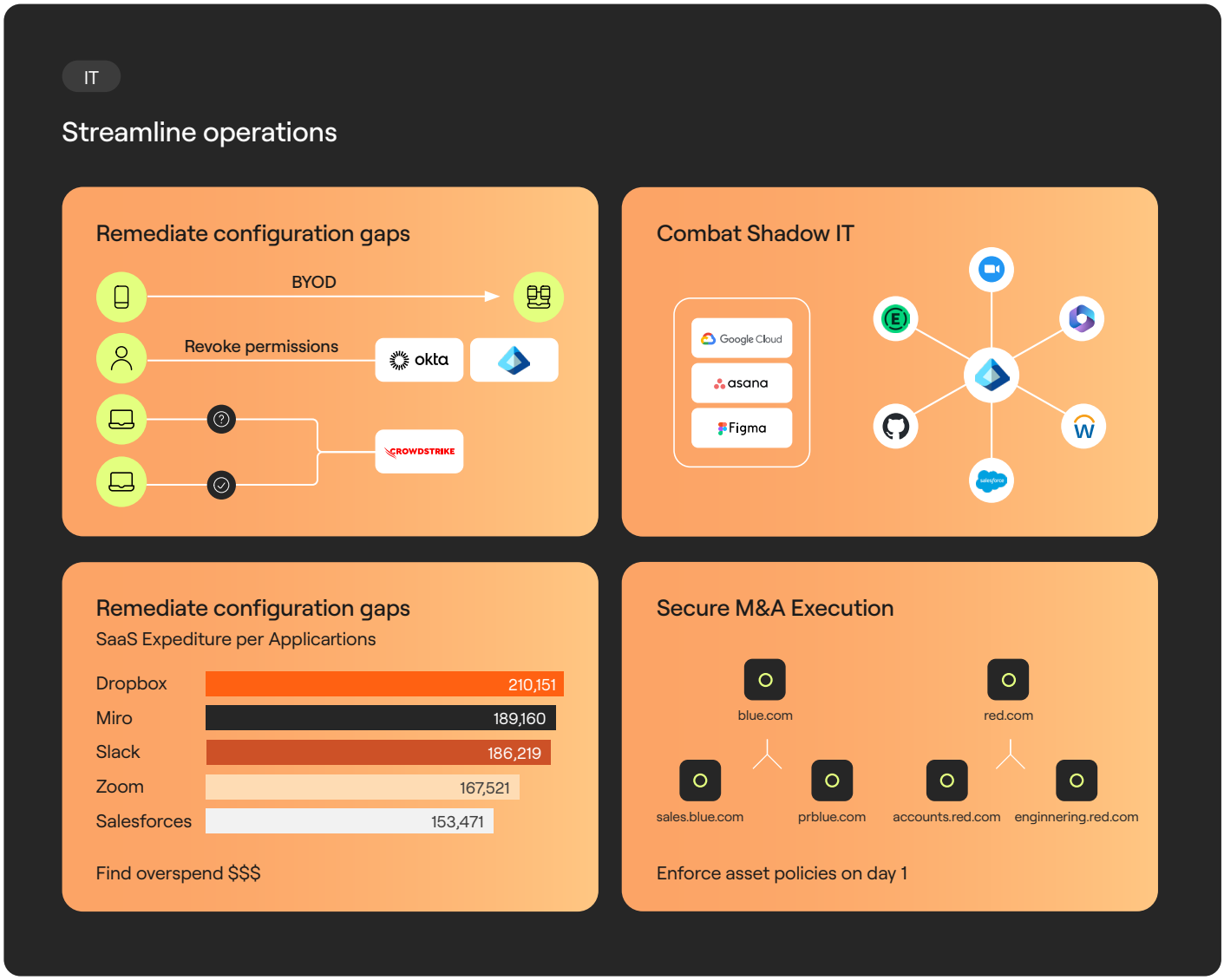
The 3 key teams you need to convince

- IT Service Management and Helpdesk
- Infrastructure /IT Administration
- Enterprise Architecture

How IT teams can benefit from a new approach to cyber asset management

CAASMs aren't limited to security use cases or only relevant for security teams. Other teams in the org, including IT, can benefit from a CAASM even if they are using a CMDB, through these use cases - remediate configuration gaps, combat shadow IT, reduce SaaS license costs, secure M&A execution.

- Remediating configuration gaps - for the assets that IT doesn't manage but can still enforce policies on, utilize CAASMs to identify what those assets are. For example, you may not be able to enforce device enrollment for BYOD, but you can ensure that your SSO solution enforce MFA even on personal devices
- Combat Shadow IT - find the apps employees are using that aren't managed by IT
- Reduce SaaS license costs - identify overspend and underutilized licenses
- Secure M&A Execution - track agent coverage, AM coverage, security policy compliance on day 1



Did you know?

Many Axonius customers use ServiceNow alongside Axonius to get even greater ROI on both investments. Check out our solution brief to learn how.

"We have a *better understanding* of 'what's out there' than ever before, and can take proactive steps to mitigate any issues, vulnerabilities, or problems."

Kyle Levenick
Program Director for the IT Security & Risk team

Getting buy-in from *Security teams*

Cybersecurity has evolved to a board-level initiative for many companies - with the three primary goals of mitigating risk, limiting financial impact, and staying compliant.

Most security leaders and teams already understand the benefit of a modern platform for cyber asset attack surface management. And, security teams are typically the one driving the deployment. So, if you're reading this section, you're most likely 1)an IT leader who also leads a security function or 2)a security leader who doesn't directly own or manage the cyber asset management program within the team. Either way, we're here to help convince whoever you need that a new approach is the way to go.

The primary pushback you'll get from security teams in the process of evaluating a modern cyber asset attack surface management solution is likely going to stem from the team already having invested in "good enough" point products, or legacy products that are so entrenched, thinking about ripping those out is a nightmare. The platform approach is the way to go - one that encompasses multiple facets of cyber asset attack surface management and gives you both visibility and actionability over your cyber assets. Read on to learn more.

The security leader POV

It's 3 AM and your security team just alerted you about suspicious activity on an unknown device on your network. Was it that contractor's laptop? An overlooked Internet of Things (IoT) device? Or something more sinister? Welcome to a typical Tuesday for cybersecurity asset management.

As mentioned earlier, all security leaders understand the need for cyber asset attack surface management. Any pushback you get is largely going to be a result of having to repurpose time, money, and resources from an existing tool to a new one. Alternatively, sometimes it's tough to prioritize cyber asset management over the hundreds of other projects underway. The best way to position investing in a more modern approach is to start the conversation with focusing on business goals around risk mitigation, financial impact, and compliance - which one matters the most to the leader you'respeaking with?

The talk track

- Managing the scope of our cyber assets has become a moving target - we have such an influx of asset types (devices, infrastructure, identities including non-human identities, SaaS apps, AI tools etc) that aren't being discovered by our existing solution
- Let's look at consolidating how we discover assets into a platform that can help us with vulnerability/exposure management, software and SaaS app posture, identity posture, and remediation
- Ideally, all of IT and Security can use this single platform as the source of truth for identifying both known and unknown devices - we can also hook into existing SecOps tools like <insert yours here - PagerDuty, Exabeam etc> and even ServiceNow for ticketing

Teams in the security org

- Infrastructure and Data Protection
- IAM
- Network Security
- Governance, Risk, Compliance (GRC)
- Security Operations Center
- Offensive Security

How security teams can benefit from a new approach to cyber asset management

For security teams, CAASMs help to minimize your attack surface. Using a CAASM like Axonius, you can:

- Manage and optimize your assets - get complete visibility over all your asset types. We talked earlier about the categories of things you control, things you can't control (but should), and things you can't control - Axonius gives you visibility into all of it
- Prioritize and remediate vulnerabilities - pinpoint the vulnerabilities that pose actual risk
- Accelerate incident response - triage faster, remediate faster

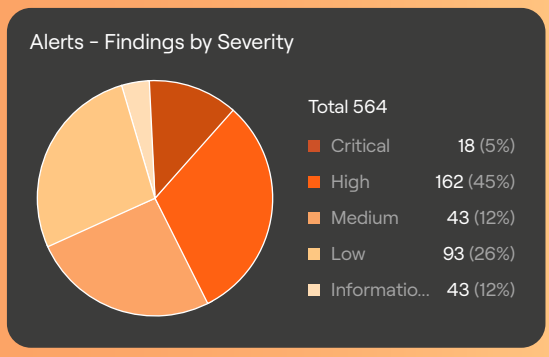
Security

Minimize the attack surface

Manage and optimize assets

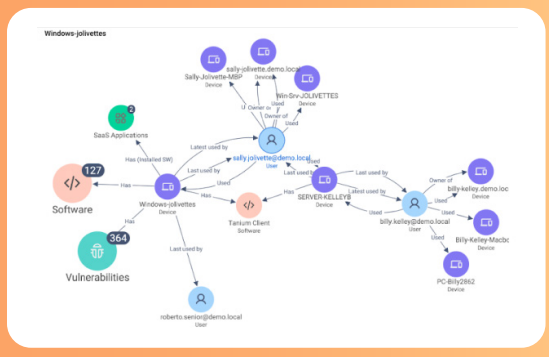
Devices | Infrastructure | Apps | Networks | Users | Known | Managed | Unmanaged (BYOD) | Unknown

Prioritize and remediate vulnerabilities



Identify the vulns that pose actual risk

Accelerate incident response



Faster triage and remediation

Did you know?

Only 17% of organizations can clearly identify and inventory a majority (95% or more) of their assets

2024 Gartner Innovation Insight: Attack Surface Management

"Being able to show our threat landscape in real time, deliver insight into our assets, and uncover security tooling helped us gather more investment to reduce risk across the organization."

Chaim Mazal
Chief Security Officer

Intro to Axonius

If you've gotten this far, cyber asset attack surface management is top of mind for you.

Let's get into how Axonius can help.

Organizations often attempt to manage complexity through a patchwork of point solutions, spreadsheets, and manual processes. This usually leads to:

- Shadow IT proliferates across departments
- IoT devices multiply without proper oversight
- Cloud assets spawn and disappear within hours
- Remote work has shattered traditional network boundaries
- Thousands of vulnerabilities are found each year, but prioritization of critical vulnerabilities is elusive

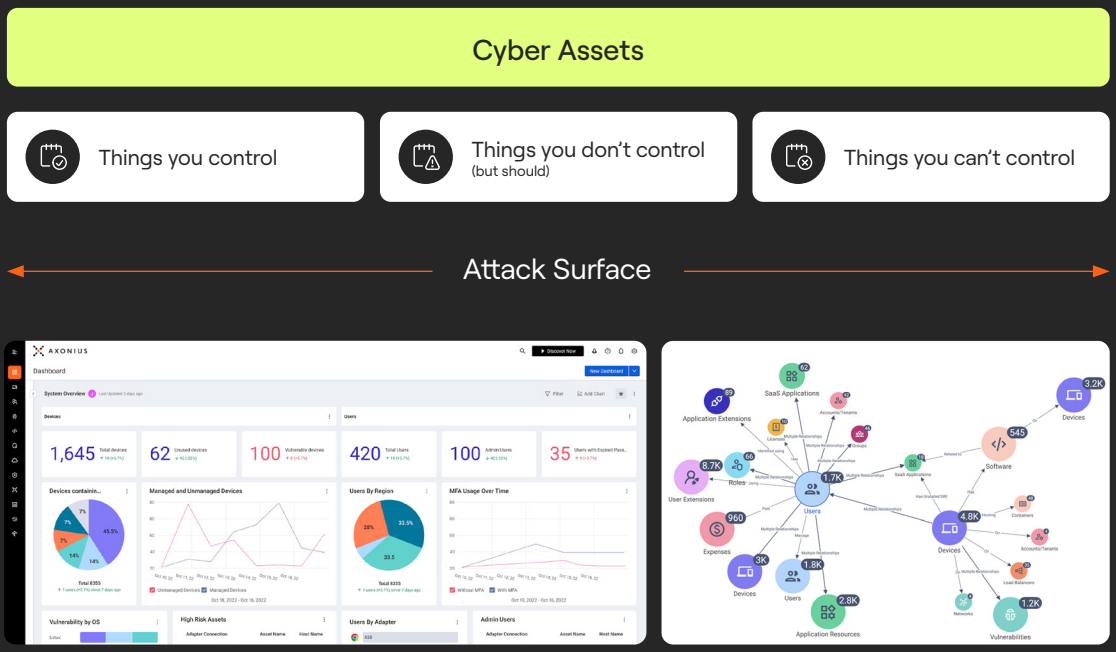
- Average cost of a data breach: $5M
- Mean time to identify a breach: 287 days
- 60% of breaches involve unpatched vulnerabilities in unknown assets

IBM Cost of a Data Breach Report

Today's security teams face a triple threat:

1. Explosive Growth: In 2025, connected devices will exceed 75 billion globally (NCCoE)
2. Tool Sprawl: Organizations manage an average of 76 security tools (Panseer)
3. Resource Constraints: 61% of firms report cybersecurity staffing shortages (ISACA)

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



Remember that time you tried to manually manage your company's assets (maybe as you're reading this)? You're probably still recovering from the nightmare.

Axonius helps you get a grip on all the assets across your entire technology footprint, and then we turn that intelligence into meaningful action.

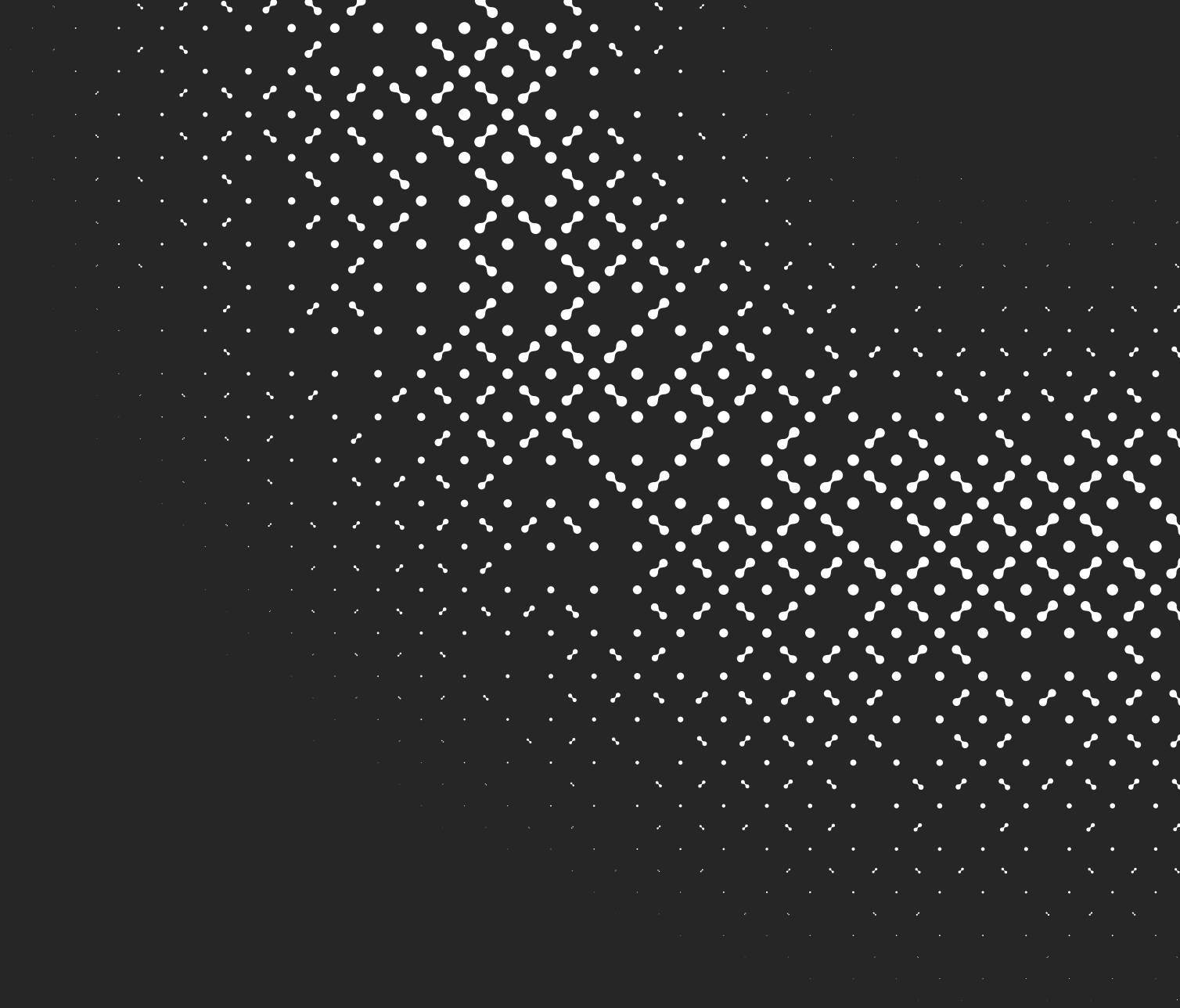
The real challenge today isn't just seeing everything, it's knowing what to do next and why. Exposures, misconfigurations, and inefficiencies inevitably happen every day because everything is so distributed - both in the cloud and physically. That's where we come in.

Forget the static inventories, disjointed tools, and endless guesswork – we pull asset data from all of your systems – devices, applications, identities, cloud, infrastructure, you name it – into a comprehensive platform.

We do this through our extensive catalog of Adapters, integrating bi-directionally with all of your systems and applications. Once connected, we run an extensive correlation and enrichment pipeline to ensure all asset data is complete, accurate, and always up-to-date.

The data model provides total visibility across your attack surface, but we don't stop there – clean asset data unlocks laser sharp actionability that has been impossible to fully realize before due to siloed systems. Operational teams gain a centralized platform that covers the end-to-end lifecycle of cyber assets, software assets, SaaS applications, identities, infrastructure, and more.

The result? Coverage gaps, critical vulnerabilities, risky misconfigurations, excessive spending, and data blind spots are illuminated and optimized before they become issues.



Axonius transforms asset intelligence into intelligent action.

Preemptively tackle hard-to-spot threat exposures, misconfigurations, and inefficiencies across your entire technology footprint – all in one place backed by one asset data model.

The actionability era of cybersecurity is here – time to bring truth to action with Axonius.

Learn more at www.axonius.com.

Axonius