AXONIUS

The State of Cyber Resilience:

Why IT and security leaders are bolstering cyber resilience as complexity increases

Introduction

It's no secret that the IT and security industry is evolving at breakneck speed.

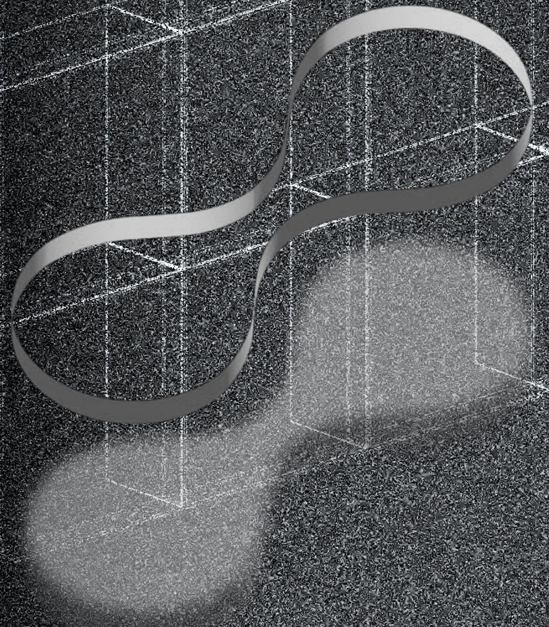
From the surge in digital transformation efforts, to shifts in work environments, and of course, increasing cyber threats, a lot has changed in the last few years — and teams are facing more complexity than ever.

Changes in the way we work may not be unusual — but the subsequent increase in digital infrastructure, attack surfaces, and the sophistication of cyber threats are. And pausing business operations because of a cyber incident can lead to significant ramifications.

The cost of cybercrime is predicted to rise to **$23.84 trillion globally** by 2027 — underscoring not only the financial burden of an attack, but the need to implement systems and processes to protect an organization's operations and revenue streams before, during, and after a cyber incident.

So, what are IT and security teams to do? How can they adapt to and strengthen digital environments in these new conditions — and combat the consequences of the expanding threat landscape?

Two words: **cyber resilience**.

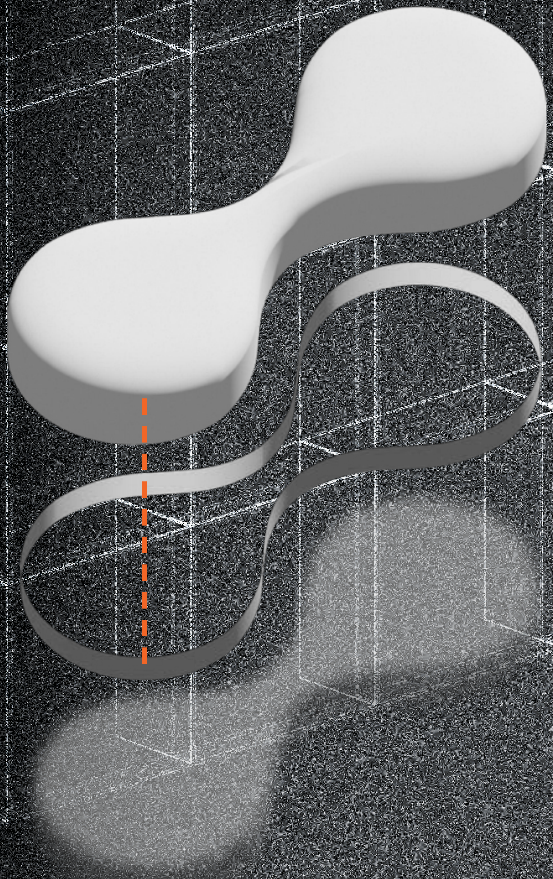


Cyber resilience is defined as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources” — and it’s a concept that’s been around for decades.

In February 2024, Axonius conducted a survey of 500 IT and security decision-makers across the United States, and found that:

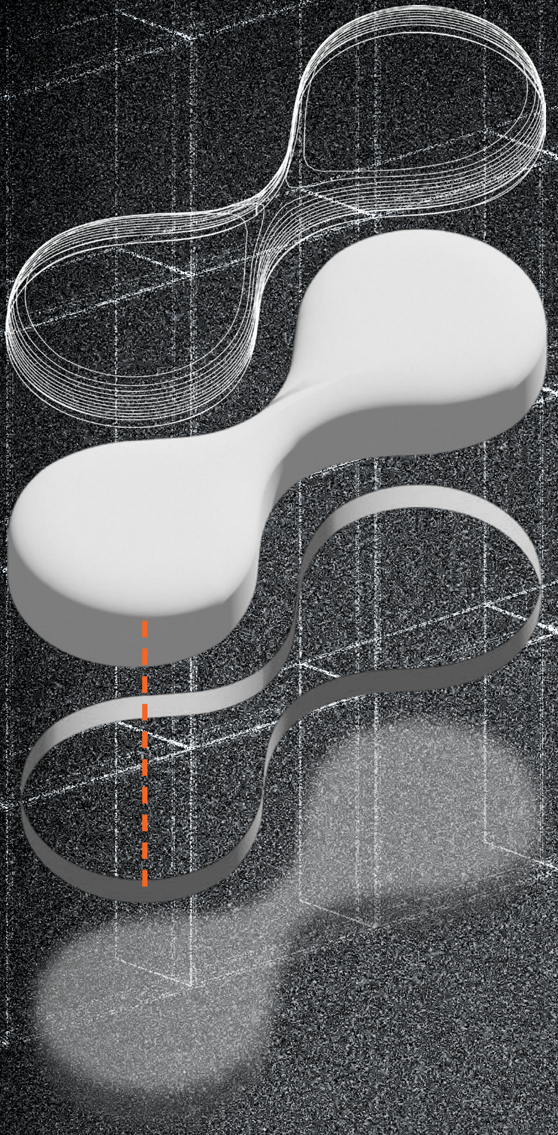
- **Cyber resilience is top-of-mind for IT and security leaders and organizations have plans to strengthen their strategies even more this year.**
- **IT and security leaders are building cyber resilience to combat external threats like cloud and network security risk and ease internal challenges such as staffing issues and resource constraints.**
- **Organizations are planning to improve their cyber resilience by investing in tools like CAASM, cloud security solutions, and more over the next year.**

In this ebook, we’ll reveal the current State of Cyber Resilience in 2024 and analyze how IT and security leaders are finding ways to bolster their ability to anticipate incidents and operate under duress as reliance on technology deepens, complexity increases, and the overall IT and security landscape evolves.



Readers will learn how they can leverage Axonius to form the solid foundation on which cyber resilience is built — helping them quickly adapt to change and keep their organization secure.

Increasing complexity across digital environments



We know that complexity is inevitable in the IT and security world — but the rate at which it's growing is unprecedented.

Why? Because the rate at which organizations are implementing new technology is *also* unprecedented.

Eighty-five percent of organizations identified "increased adoption of new and frontier technologies and broadening digital access" as the factors most likely to drive digital transformation initiatives across their organization, according to the 2023 **World Economic Forum Future of Jobs Report**.

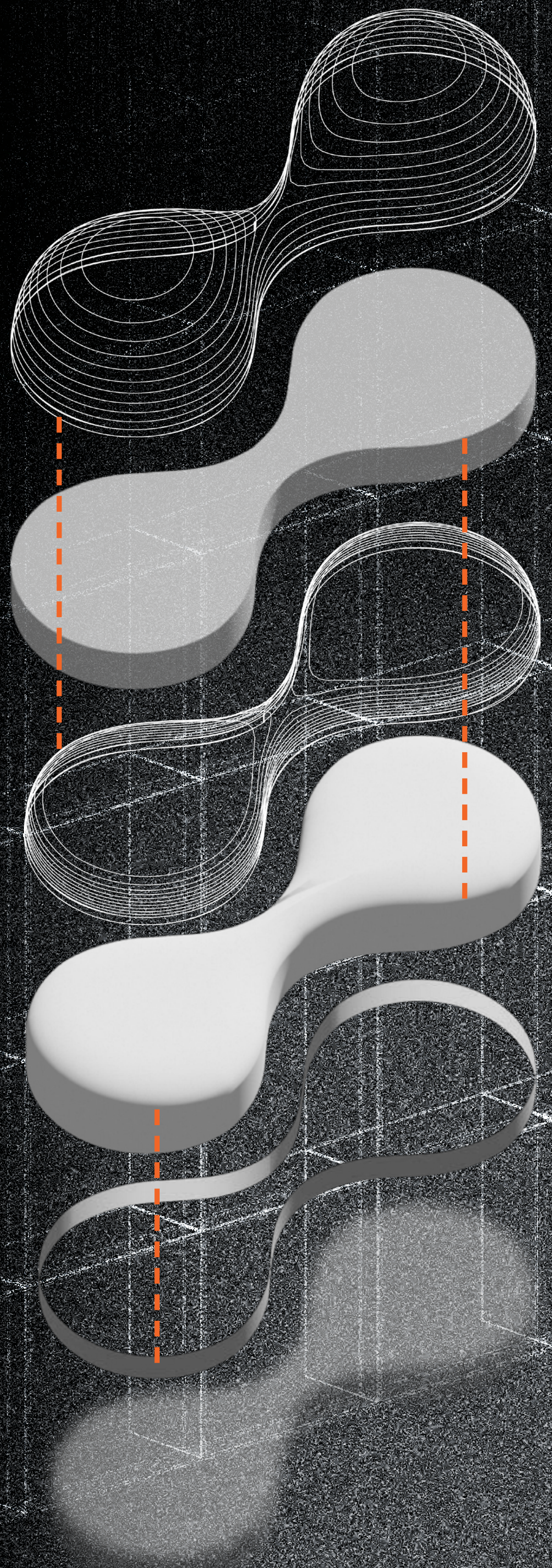
And more tech equals more complexity.

As organizations rapidly undertake more digital transformation efforts, the proliferation of devices, software-as-a-service (SaaS) apps, third-party and vendor connections, and cloud services results in diverse, and oftentimes, disparate processes and standards.

Not only are IT and security teams faced with managing constantly changing digital environments, but it's evident that meeting the demands of digitization adds time, effort, and complexity to IT and security procedures.

And with IT and security teams still facing ongoing **skill shortages**, teams are left using limited resources to manage new and compounding complexity.

How are IT and security leaders adapting?



Cyber resilience is a growing priority

Cyber resilience has evolved significantly since its emergence in the early 2000s.

As IT and security leaders transition away from perimeter and defense-based security approaches towards multi-layered strategies, they're better equipped to anticipate, prepare for, withstand, and recover from cyber incidents.

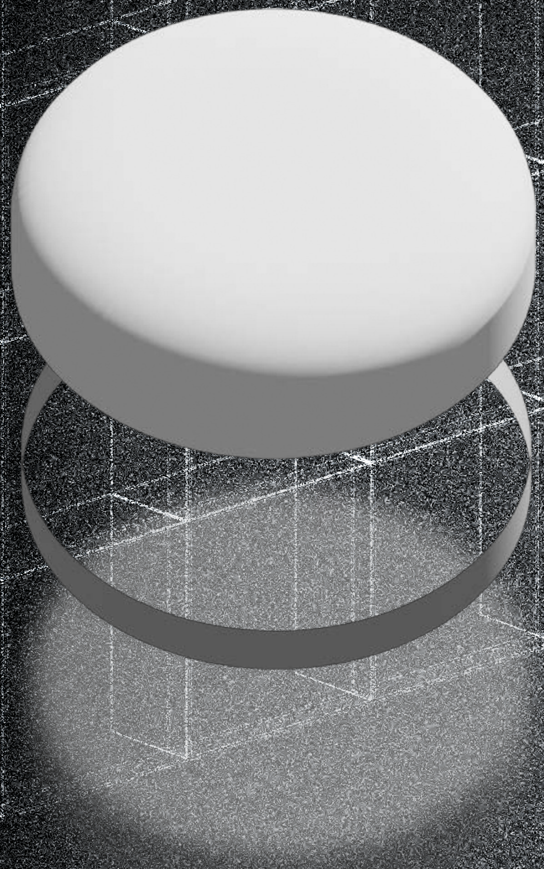
According to our data, 99% of decision-makers understand the importance of cyber resilience in reducing exposure to critical infrastructure, enhancing enterprise security posture, and ensuring compliance. And now, organizations are taking steps to build out their cyber resilience: 77% of respondents report an increase in their organization's cyber resilience over the past 12 months, and 80% anticipate further improvement in 2024.

Despite the shifts towards cyber resilience, investments to improve it are still relatively new. Nearly half (44%) of IT and security leaders say their organization started investing in cyber resilience within the last year and almost 30% only began investing in cyber resilience within the last six months.

It’s surprising that advances to improve cyber resilience are proportionately low compared to the significance IT and security professionals place on it — but our survey results found that cyber resilience is expected to grow.

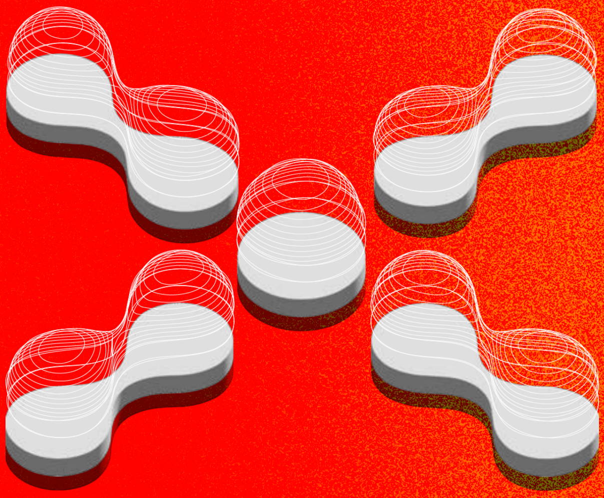
The recent resurging interest in **proactive security** provides a clue to why. The cybersecurity industry is striving to reach cyber maturity to the point where it has the technological capabilities to improve expanding attack surface security and ensure business operations remain unhindered during times of duress.

And, with organizational leadership, including boards of directors, providing an **increased emphasis on cyber resilience** as cyber-attacks become larger in scale, IT and security decision-makers rank ensuring business continuity (35%) and managing an increase in cyberattacks and cyber threats (32%) as the top two reasons they’re turning to cyber resilience.

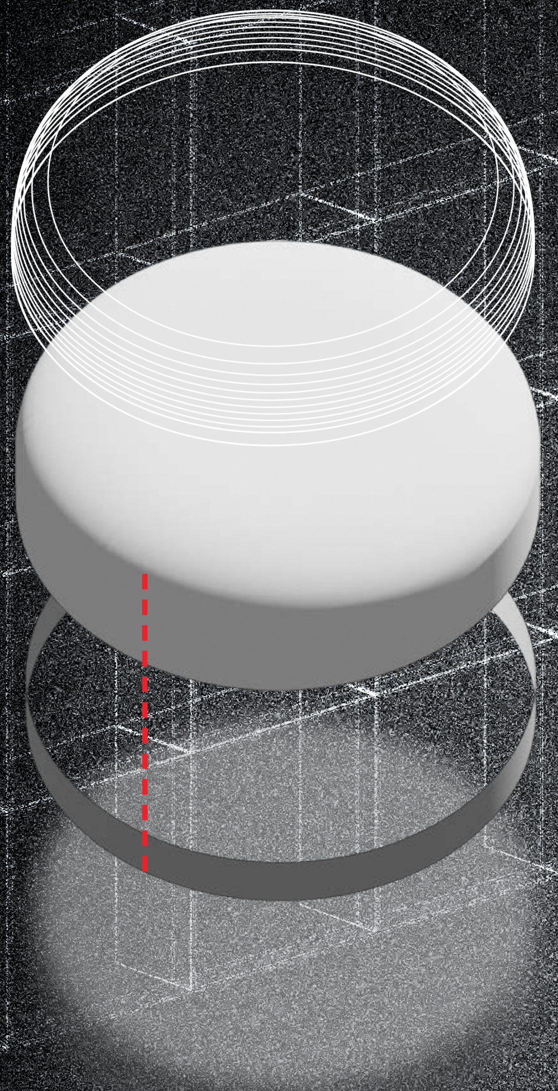


It’s time that we proactivate — which means knowing what we need to protect and what postures need to be straightened out, minimizing cracks in remediation processes, and ensuring that we have appropriate reporting.

– Erik Nost,
Senior Analyst, Forrester



Staying resilient to emerging challenges



IT and security leaders place considerable trust in their cyber resilience, with data from our report showing that 88% believe that their organization would be able to **continue operating in the event of a security incident**.

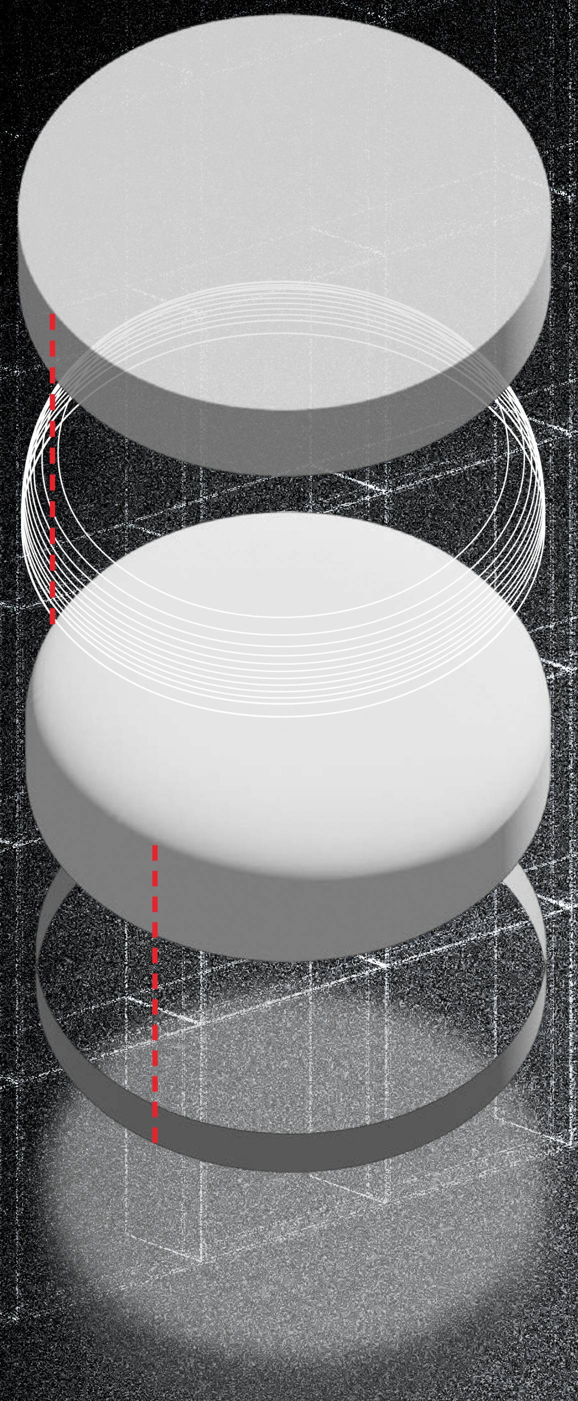
But despite their confidence, every respondent expressed concerns regarding various external and internal threats to their IT and security programs.

Let's take a closer look at those concerns.

For one, the top challenge facing teams comes down to integration issues with existing systems (26%) — a concern shared by others. We found that organizational leadership (C-suite, board of directors) also expressed integration as a challenge, citing apprehensions of compatibility with other resources and existing cybersecurity infrastructure.

As organizations rely on cloud and software-based technology to improve resilience and increase maturity, new challenges have also materialized.

The accelerated shift to multi-cloud operations has caused growing concerns about cloud security.



It's easy to see why. These days, IT and security teams now manage more than 25,000 permissions from the top three cloud service providers alone. And with organizations adopting **hundreds of SaaS apps** to improve collaboration and communication, in due course, attack surfaces have quickly expanded.

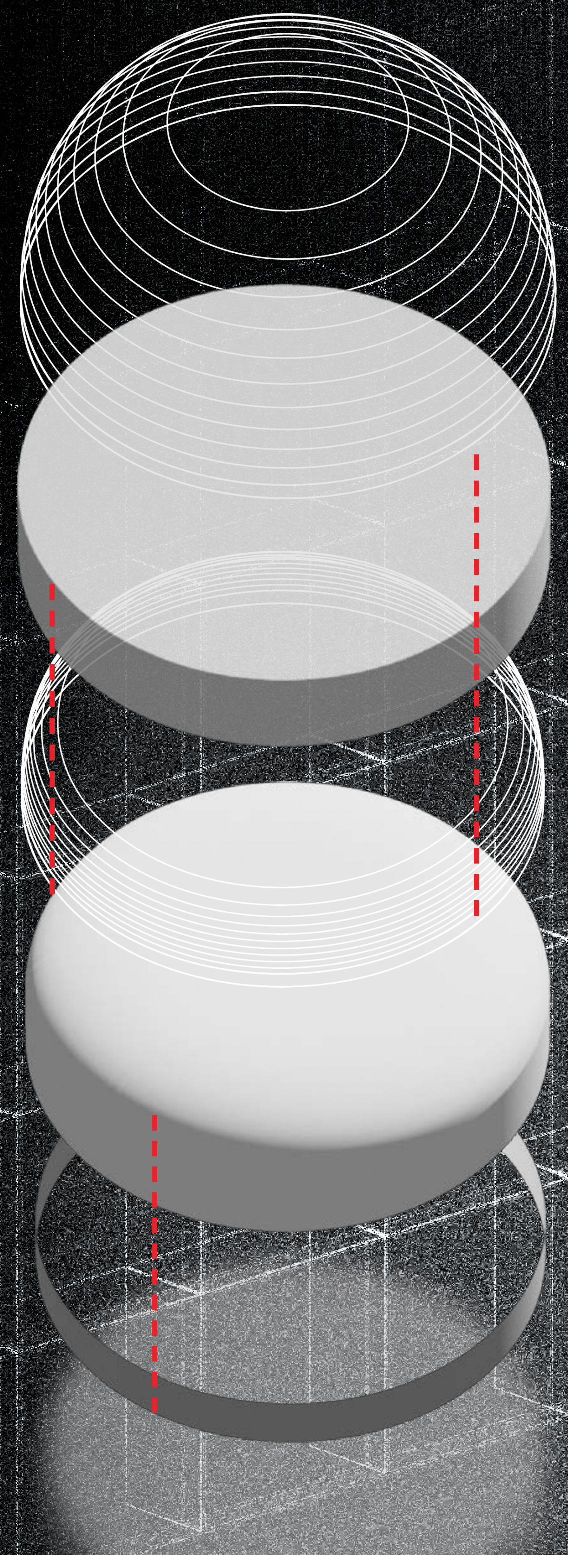
While the influx of cloud infrastructure and SaaS apps have helped organizations reduce costs, improve efficiency, and boost productivity, cloud security is listed as the top anticipated threat to cyber resilience for more than half of the IT and security decision-makers (55%) over the next 12 months.

Moreover, as security programs call for increased skills, talent, and budgets, IT and security leaders are challenged to get the most value out of their existing resources.

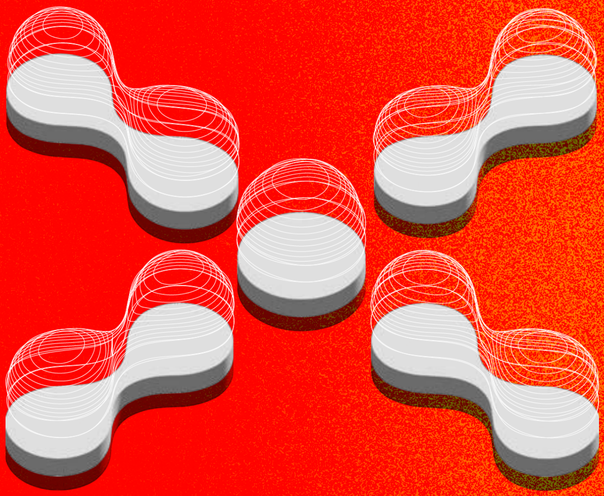
Today's cybersecurity and IT market demonstrates that the days of over-hiring and overspending are over, and IT and security leaders are feeling the strain.

Respondents cited the skills gap and staffing issues (26%), reduced IT and security budgets (25%), and lack of employee training (21%), as top threats to their cyber resilience strategies over the next year.

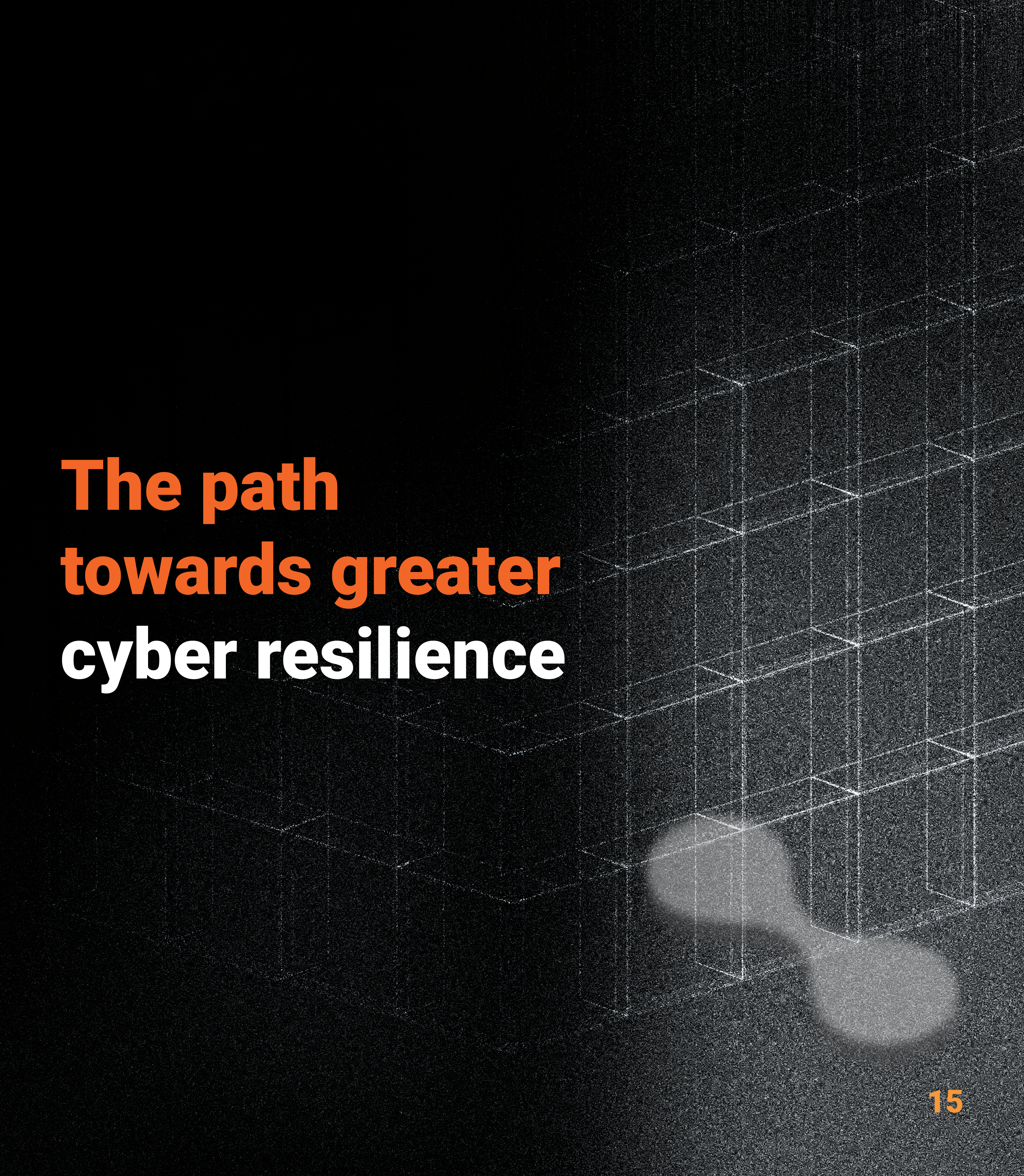
With growing apprehension about threats new (and old), this all begs the question: what does it *truly* mean to be cyber resilient?



While the influx of cloud infrastructure has helped organizations reduce costs, improve efficiency, and boost productivity, cloud security is listed as the top anticipated threat to cyber resilience for more than half of the IT and security decision-makers (55%) over the next 12 months.



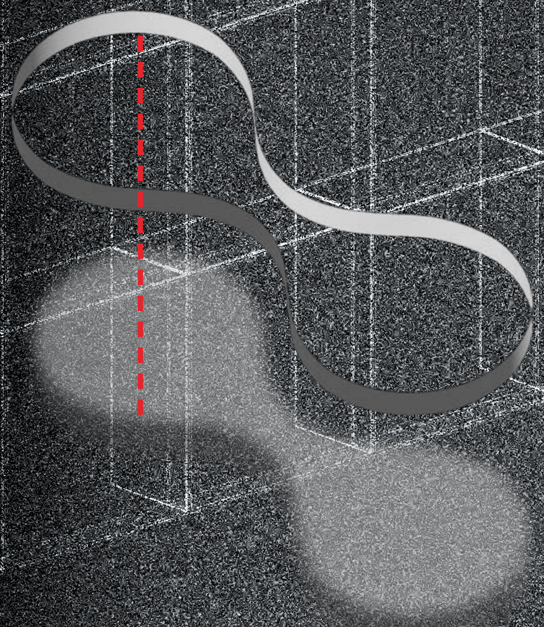
The path towards greater cyber resilience



The reality is, cyber resilience has always been a challenge to define and inevitably achieve because cybercrime is imminent, complexity is always increasing, and resilience is subjective.

What's certain, however, is that knowing and understanding what exists in the IT environment builds the foundation for securing your attack surface.

It was only a couple of years ago that **Gartner** ranked attack surface expansion as the top trend for increasing potential cyber threats — and unfortunately, this has remained true. As attack surfaces grow, lack of visibility hinders the ability to meet security and operational objectives, creating more risk. In some cases, organizations have reported **3.3 times more incidents** caused by a lack of visibility into cyber assets.



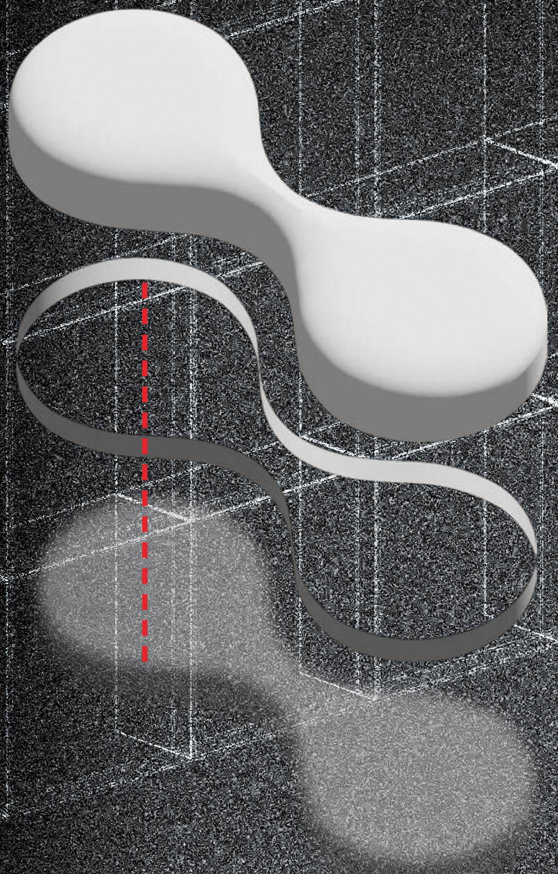
To strengthen attack surface security, in its **Top Cybersecurity Trends in 2024**, Gartner recently recommended security leaders focus more on resilience-oriented investments to enhance risk management of third-party services due to the inevitability of third parties experiencing cybersecurity incidents.

The data from our report reflects this. The top three tools IT and security leaders are investing in include cloud security solutions (54%), identity and access management tools (43%), and Cyber Asset Attack Surface Management (CAASM) solutions (41%).

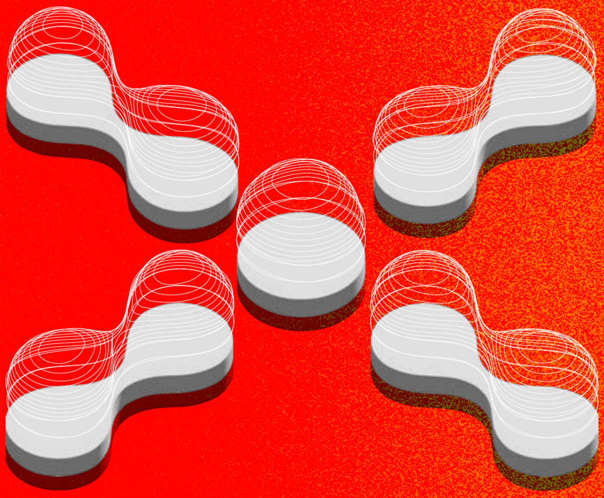
Interestingly, over 40% of respondents also reported they'll continue to use **CAASM solutions** in the future — and for good reason.

You can't secure what you don't know exists, and CAASM solutions — like the one Axonius offers — provide IT and security teams the foundational visibility they need to make smart decisions, improve resiliency, and ensure business continuity.

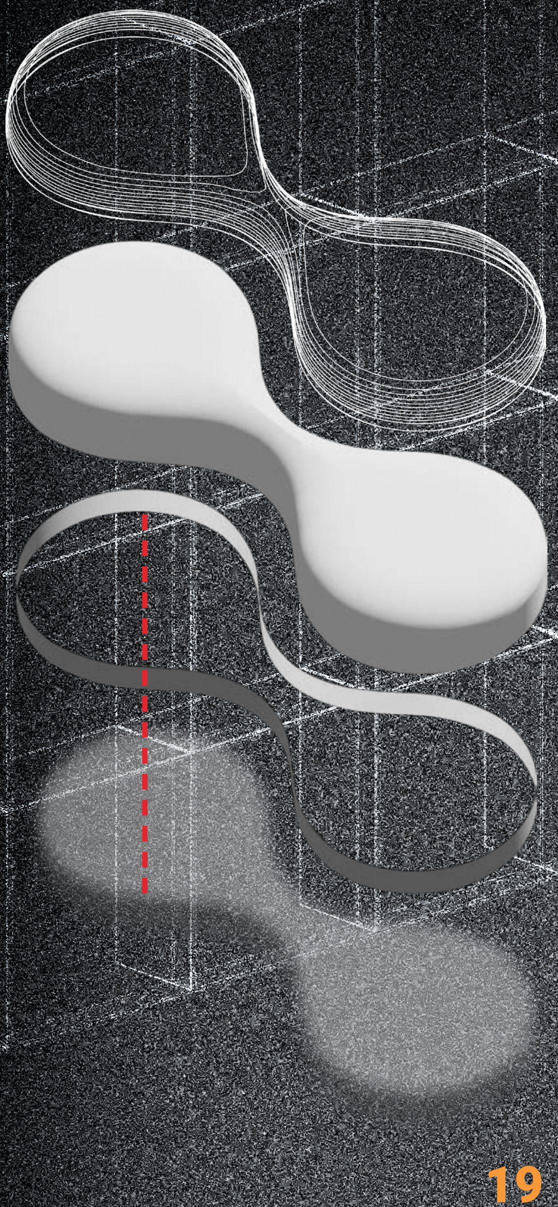
Let's dive deeper into how CAASM can help organizations improve their cyber resilience.



The reality is, cyber resilience has always been a challenge to define and inevitably achieve because cybercrime is imminent. What is certain, however, is that knowing and understanding what exists in the IT environment builds the foundation for securing your attack surface.

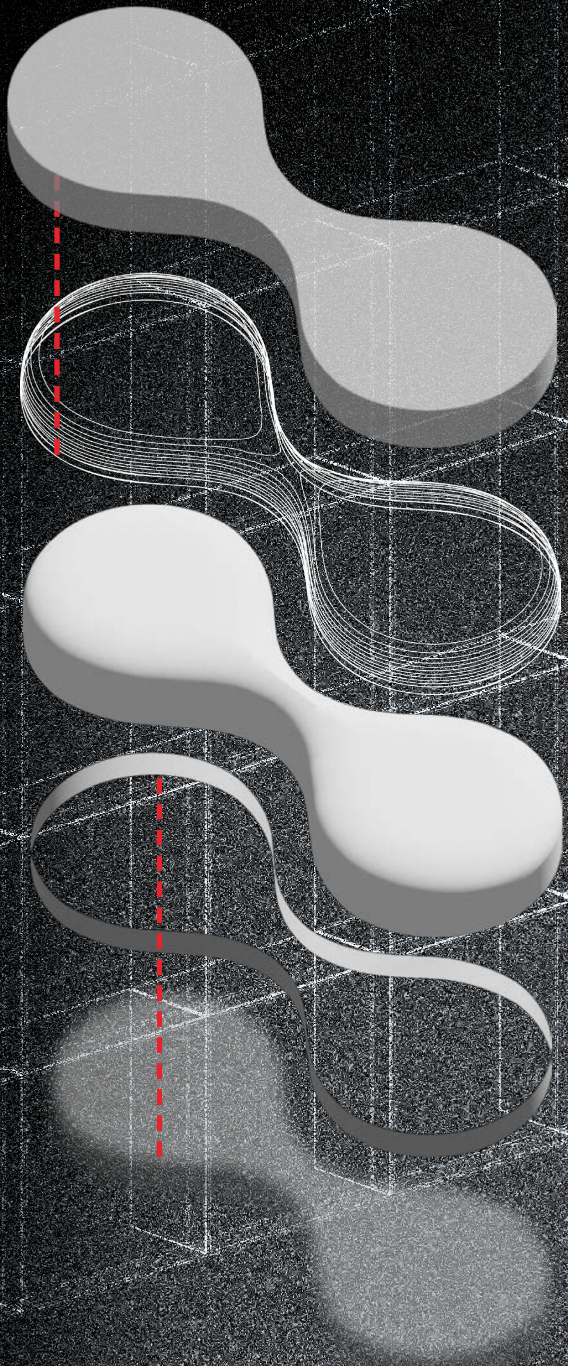


Optimizing for resiliency with CAASM

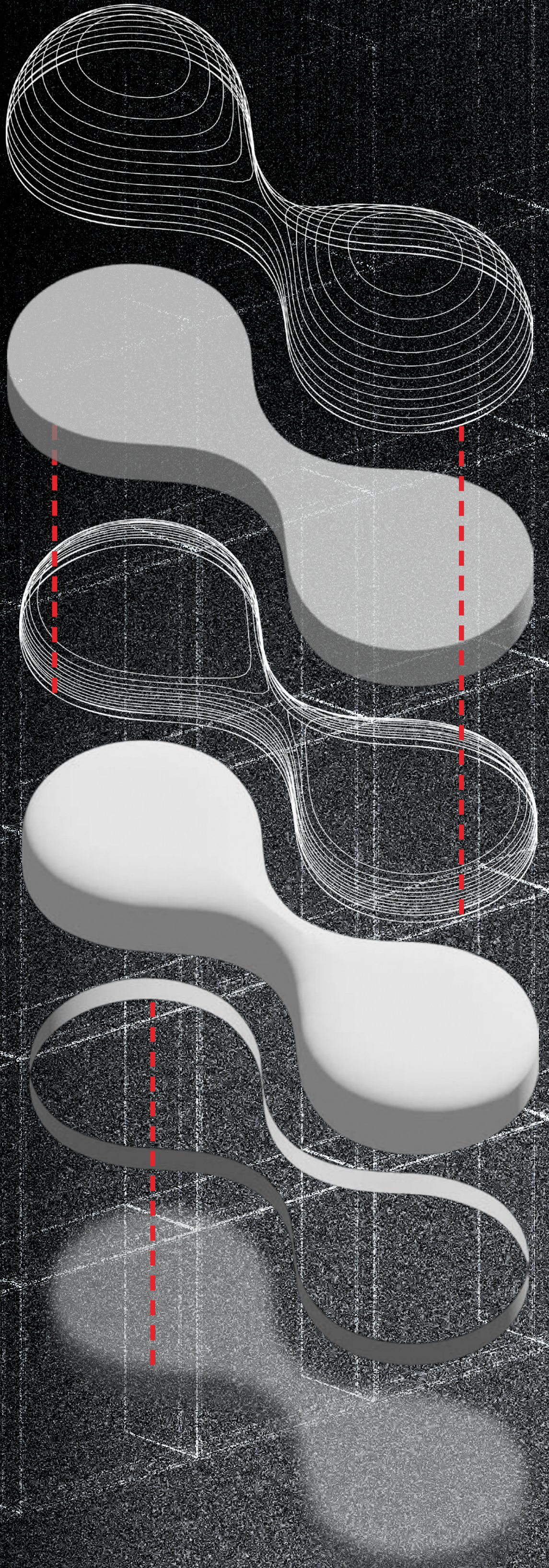


Gaining the ability to foresee, withstand, and recover from evolving cyber threats is challenging, especially when your organization has limited resources. But strengthening your cyber resiliency is critical to keeping up with today's expanding attack surfaces and growing IT and security concerns.

How can your organization optimize its resources to strengthen resilience? Here are three steps to help your team, starting with building a foundation.



1. Establish your foundation



Plain and simple, you can't build anything without a foundation. For IT and security, that foundation means **knowing and understanding what exists in the IT environment**.

From managing newly added devices to onboarded software and cloud-based SaaS assets, complete visibility has become fundamental to understanding what to secure — and ultimately, improving cyber resilience.

A CAASM solution like Axonius offers the foundation IT and security teams need to bolster resilience by providing comprehensive and contextual visibility into all assets. For organizations trying to account for software and cloud-based assets, discover unmanaged devices, monitor legacy or outdated infrastructure, or identify all internet-connected devices, Axonius spans from devices and users across the digital environment, regardless of location, uptime, or power state.

For IT and security teams, understanding the context of digital infrastructure is now critical to inform strategies and make data-driven decisions to improve asset and attack surface security.

2. Evaluate your processes and defenses

No matter how resilient you think your organization is, cyber attacks are constantly evolving. So, enough is **never truly enough**. Staying on top of emerging threats requires ongoing assessment of processes, defenses, and the state of the attack surface.

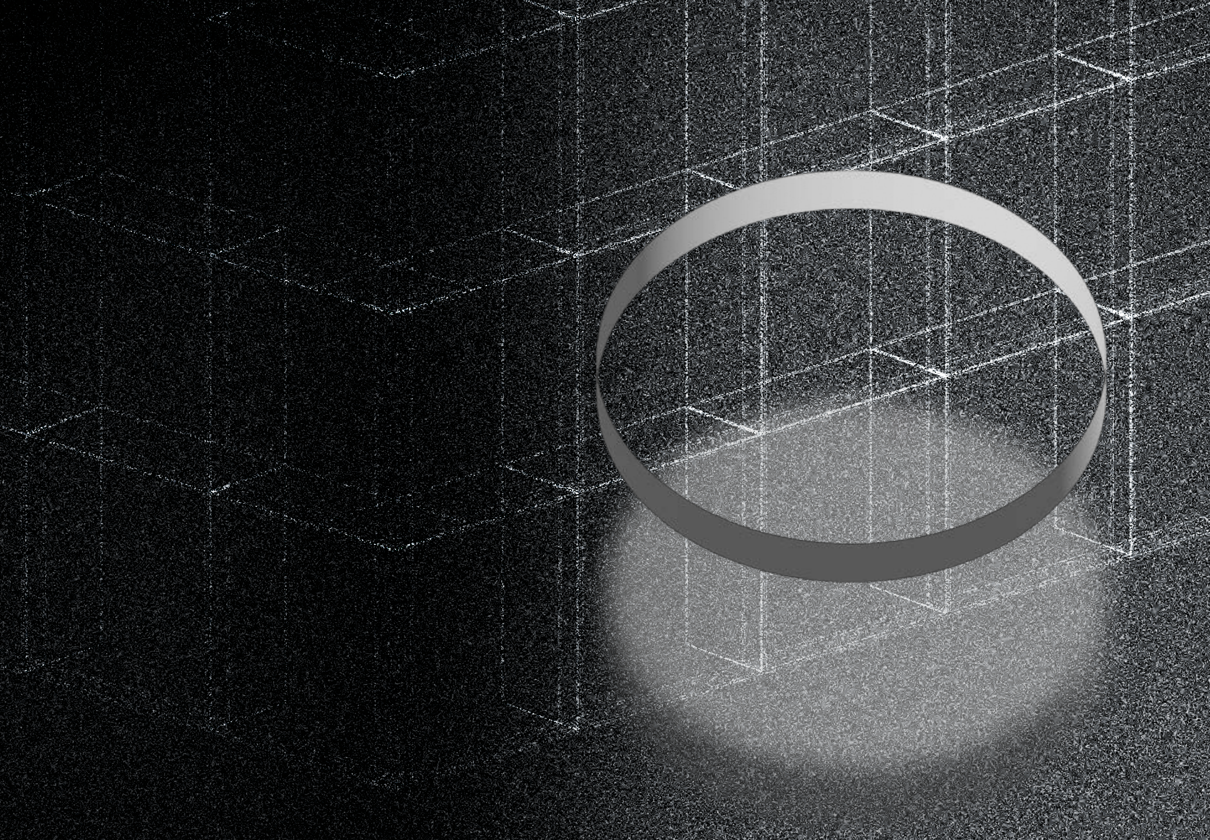
When evaluating the attack surface, identify which challenges are most susceptible to impact business operations during an attack, and how to mitigate them.

Let’s look at a few processes and how Axonius helps support IT and security teams to strengthen them.

Cloud security:

Cloud migration is skyrocketing – with **90% of large enterprises** now using multi-cloud infrastructure. But, as cloud migration continues across organizations, cloud security is a growing concern.

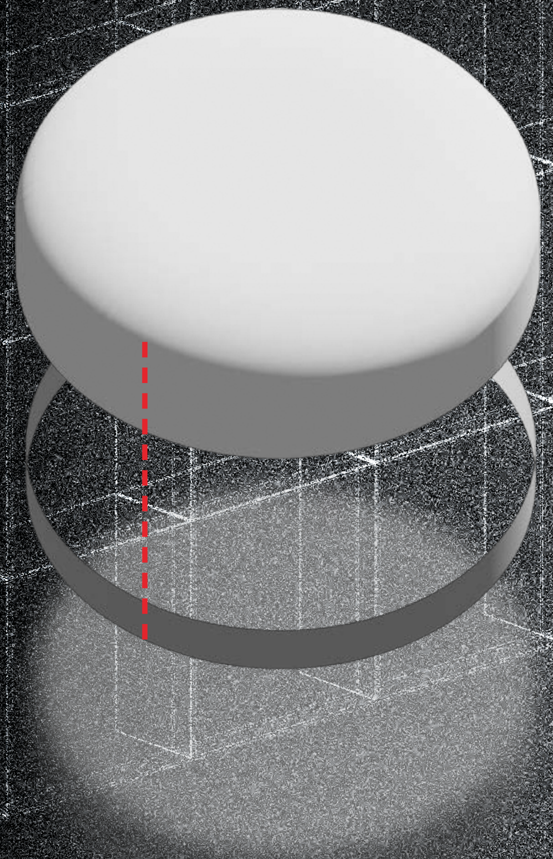
Axonius helps IT and security teams strengthen cloud security posture by improving cloud security visibility. From managing vulnerabilities to tracking and bolstering cloud compliance, Axonius offers the insight needed to be proactive about cyber risk management.



Vulnerability management:

Resource-restricted IT and security teams often struggle to understand the prevalence of vulnerabilities, **identify threats**, and reduce the attack surface.

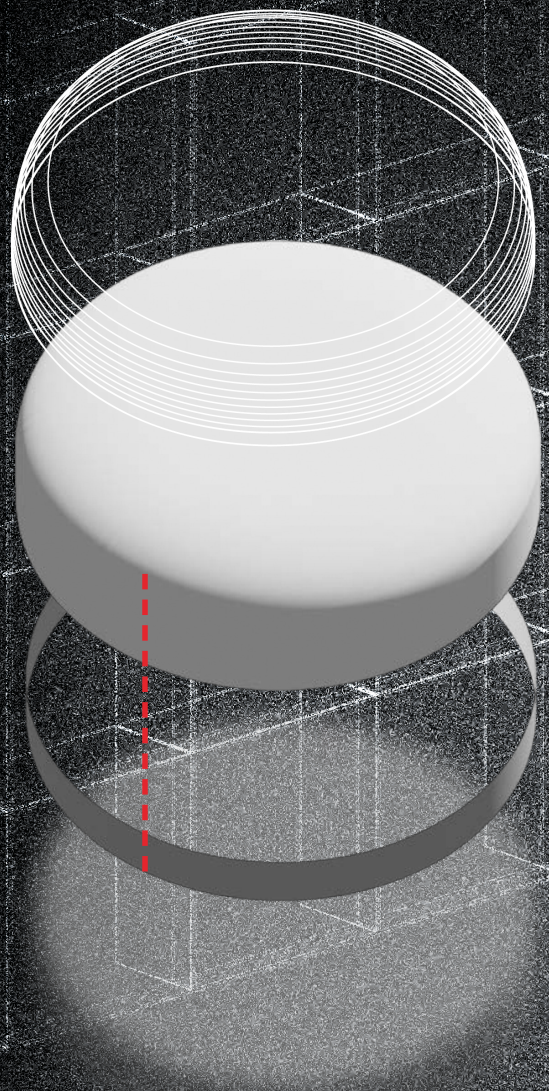
Axonius addresses vulnerability management issues head-on. It delivers automated visibility into cybersecurity vulnerabilities and offers a holistic view of threats, allowing IT and security teams to identify vulnerabilities across entire fleets of devices and then prioritize and remediate based on urgency and importance — expediting patching and remediation processes.



Software management:

Software is a struggle to identify because of today’s **dynamic** IT environment, especially if it hasn’t been properly vetted — including instances of software running on mobile and BYOD devices that connect and leave networks frequently.

For IT and security, Axonius sheds light on unauthorized, unwanted, or suspicious software, and makes it easy to uncover security gaps such as end-of-support or end-of-life software that no longer provides updates or patches and puts your environment at risk.



SaaS management:

SaaS adoption has exploded in the last few years. With organizations using **87 SaaS apps** on average, IT and security teams are challenged with managing configuration issues, unsanctioned, unmanaged, and shadow SaaS apps.

And, as more employees are onboarded and collaboration, efficiency, and communication needs expand across organizations, understanding where SaaS apps live, who owns them, and the context behind them can get complicated.

Axonius reduces SaaS complexity and allows teams to discover all known and unknown SaaS applications. Allowing IT and security professionals to assess, address, and mitigate SaaS risk, Axonius discovers and mitigates configuration issues, identifies data security risks, and delivers contextual insights for better IT management.

3. Educate and automate

Time, effort, and resources are stretched thin in today's modern IT and security landscape. With the ongoing skills shortage impacting teams' efficiency and productivity, it's more important than ever to get the most value out of **your most important asset** — your people.

Providing upskilling and training development opportunities can be an effective tactic to help your team learn new skills and reduce the effects of burnout. But security training and development should span beyond the IT and security department and be integrated across an organization.

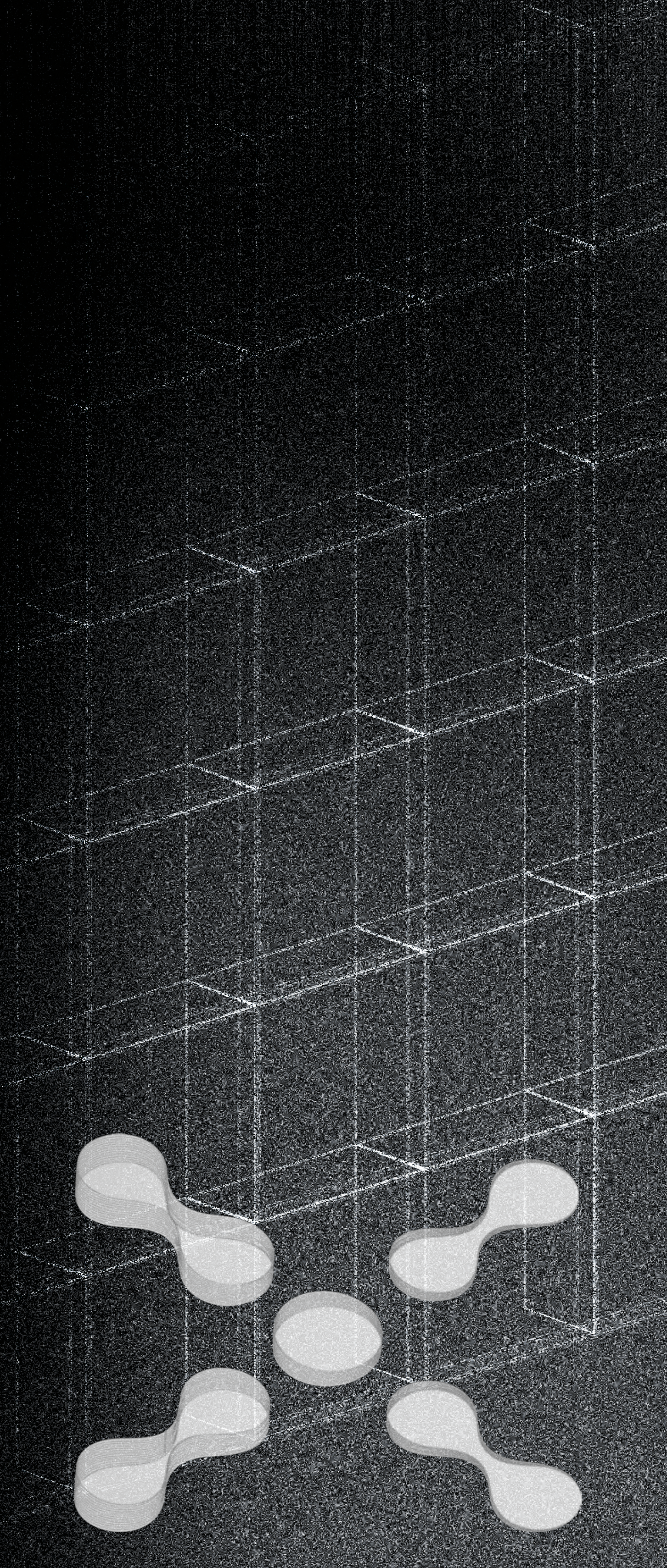
Like broader company culture, teams share cybersecurity responsibilities, and implementing clearly defined security protocols, standards, and cyber education throughout an employee's tenure can help ensure everyone can contribute to building cyber resilience from day one.

If your team is spending the bulk of its time on tedious and manual tasks, there's little to no time left for strategy and preparation. Eliminating manual processes and implementing tools that enable automation can increase productivity, efficiency, and create opportunities for strategic tasks.

Take vulnerability management, for example. While it's critical to improving resilience strategies, correlating assets to known vulnerabilities, remediating them, and then double-checking to ensure everything's been patched can be a difficult, rigorous, and oftentimes, error-prone task to do manually. Employing an automated system can quickly correlate information from disparate sources and assets, including those IT are unaware of.

Axonius uses non-intrusive API-based adapters to bring in context from hundreds of different data sources. Data is automatically normalized and de-duplicated, creating a comprehensive, single source of truth for all assets. This process simplifies asset and vulnerability management so that teams can quickly collect accurate information and keep to timetables like those from different frameworks.

Building cyber resilience must work to relieve the concerns organizational leaders have — from resource constraints to time constrictions — and automation can efficiently and effectively leverage skills for ensuring business continuity versus focusing on manual tasks.

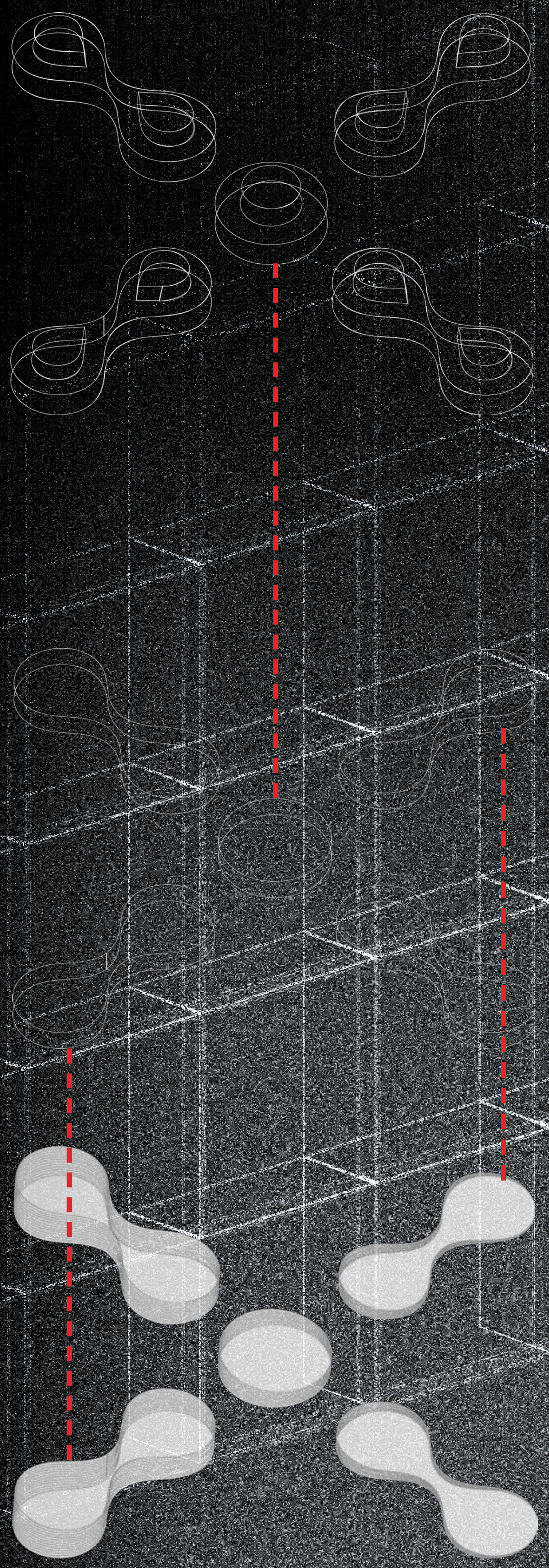


Controlling the complexity of modern challenges and cyber resiliency threats

For IT and security leaders, a comprehensive view of tech stacks, such as the one provided by Axonius, allows them to gain the insights they need to make decisions that foster business continuity and growth and control ongoing complexity.

Axonius provides a complete view into the tools and solutions IT and security teams are using, identifies gaps that need to be filled, and offers insight into what's new, not in compliance, or underutilized. This gives leaders a leg up in optimizing their teams and resources, and improving cyber resilience, despite the challenges they may face.

With a **solid foundation** to understand the entire IT environment, organizations can quickly adapt to challenges and leverage insights to prepare for future cyber threats or incidents.



AXONIUS

AXONIUS.COM

Axonius gives customers the confidence to Control Complexity™ by mitigating threats, navigating risk, automating response actions, and informing business-level strategy. With solutions for both cyber asset attack surface management (CAASM) and SaaS management, Axonius is deployed in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically validate and enforce policies. Cited as one of the fastest-growing cybersecurity startups, with accolades from CNBC, Forbes, and Fortune, Axonius covers millions of assets, including devices and cloud assets, user accounts, and SaaS applications, for customers around the world.

330 Madison Ave, 39th Floor
New York, NY 10017
info@axonius.com