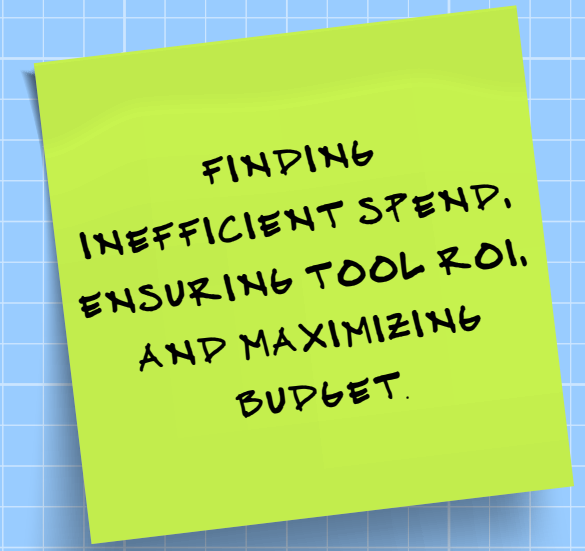
COST OPTIMIZATION:

The Consensus IT and Cybersecurity Priority



AXONIUS

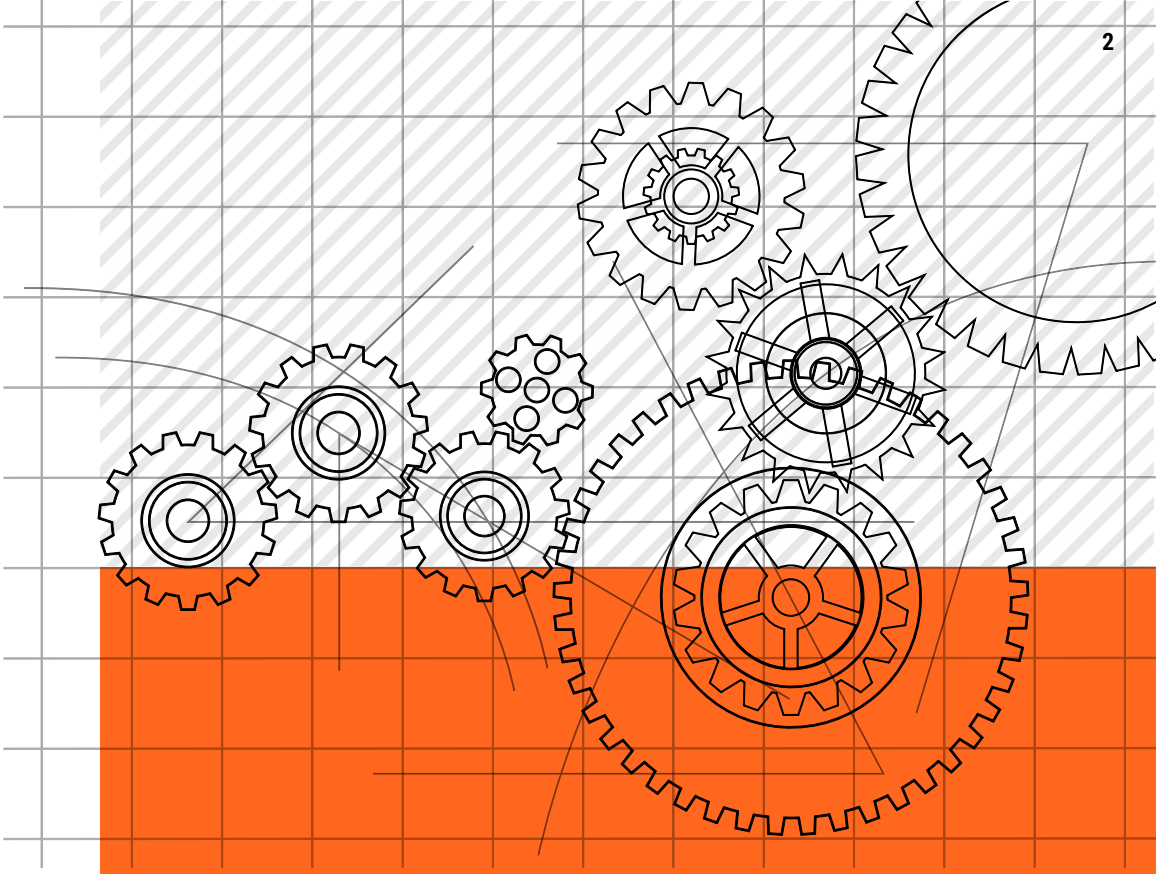
In recent years, security and IT teams were flush with cash. The focus was on initiatives, like building a digital infrastructure and connecting remote workforces. The need for subscription and cloud-based products soared. IT budgets grew at their fastest rates in over 10 years[1].

Then a reality check came in a *big* way.

Economic uncertainty has tamped down the financial spigot. For many organizations, budgets in nearly every department — including IT and security — are under scrutiny. CIOs and CFOs are reassessing what tech investments to make or cut. Because of this, IT and cybersecurity teams are being forced to slash spend, and are looking at ways to get "more bang for their buck" to fund priorities going forward.

With smaller budgets and less staff, IT and cybersecurity teams must find ways to automate manual, time-consuming, and low-value tasks. At the same time, simply buying more solutions to solve the problem isn't an option. Instead, IT and cybersecurity teams must look inward at existing tools and assets to better understand deployment, usage, and value.

But how do IT and cybersecurity leaders find inefficient spend and complete high-priority projects with limited budgets — and even smaller teams?



READ ON TO LEARN:

- The types of cost inefficiencies IT and security professionals face
- Ways to optimize cost and show ROI
- How a modern, comprehensive approach to cybersecurity asset inventory helps deliver on cost optimization while continuing to protect an organization's attack surface

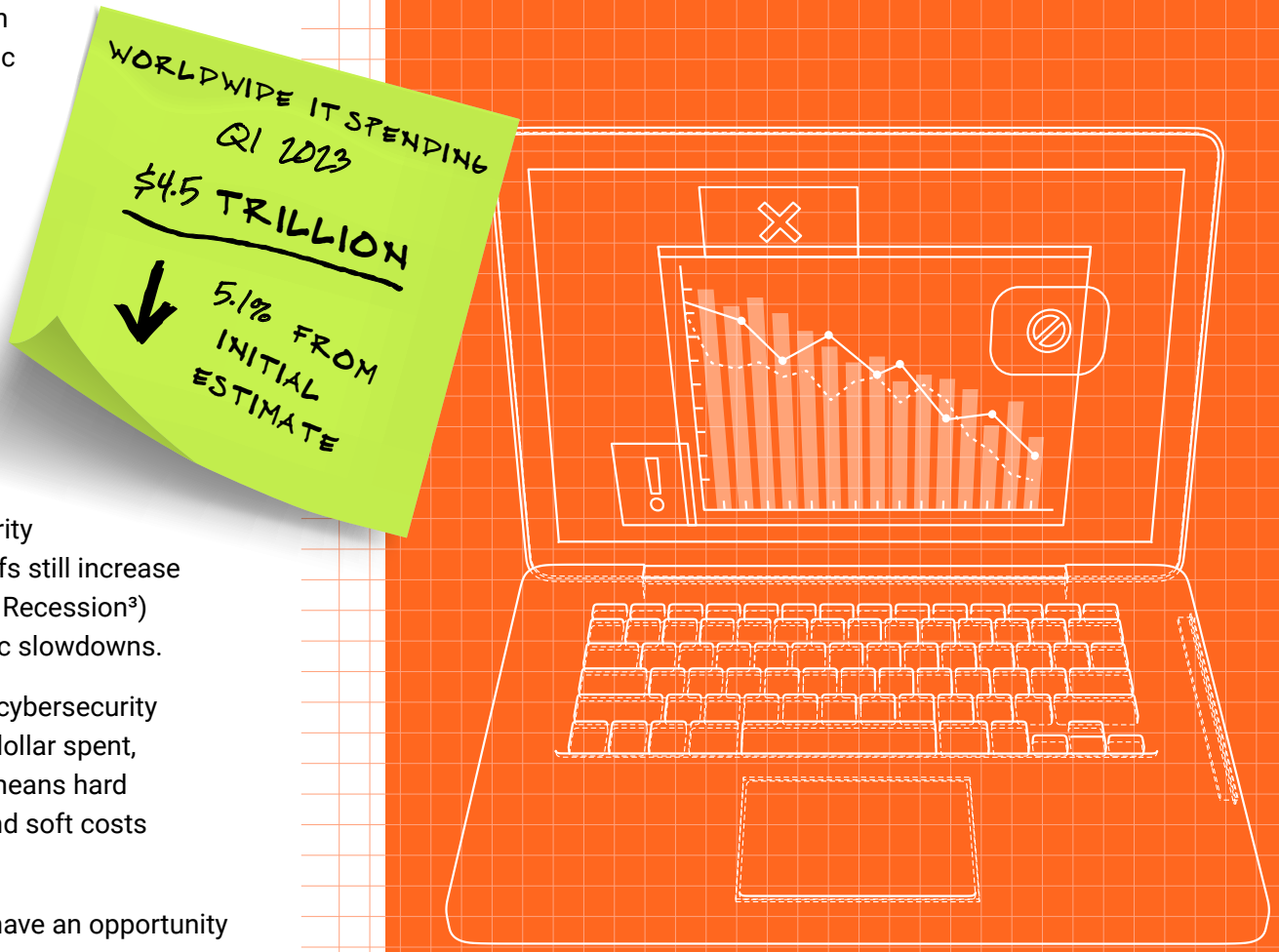
1 "IT Budgets Are Growing. Here's Where the Money's Going", Gartner, October 21, 2021.

IDENTIFYING COST INEFFICIENCIES

Making the Case for Cost Optimization

The cybersecurity industry is resilient — even in tough financial times. But with recent economic headwinds, overall tech spending is slowing down and budgets are getting even tighter.

Worldwide IT spending is expected to total $4.5 trillion in 2023, a slight increase of 2.4% from 2022. That's down from Gartner's initial estimate of 5.1% growth for 2023[2].



Lower budgets are also resulting in smaller headcounts. According to widespread reports, over 400 tech companies laid off more than 122,000 employees in the first quarter of 2023 alone. Even though cybersecurity professionals have largely been immune, layoffs still increase security risk. Historical events (think the Great Recession[3]) show cybercrime often spikes during economic slowdowns.

To avoid further headcount reductions, IT and cybersecurity leaders are putting a renewed focus on every dollar spent, including identifying cost inefficiencies. That means hard costs (like equipment or software licenses), and soft costs (think manual processes or human capital).

By discovering where hidden costs lie, teams have an opportunity to decrease spending all around. And by recovering much-needed budget dollars from assets that aren't being used or showing ROI, unrealized spend can be shifted to better use.

2 "Gartner Forecasts Worldwide IT Spending to Grow 2.4% in 2023", Gartner, January 18, 2023.

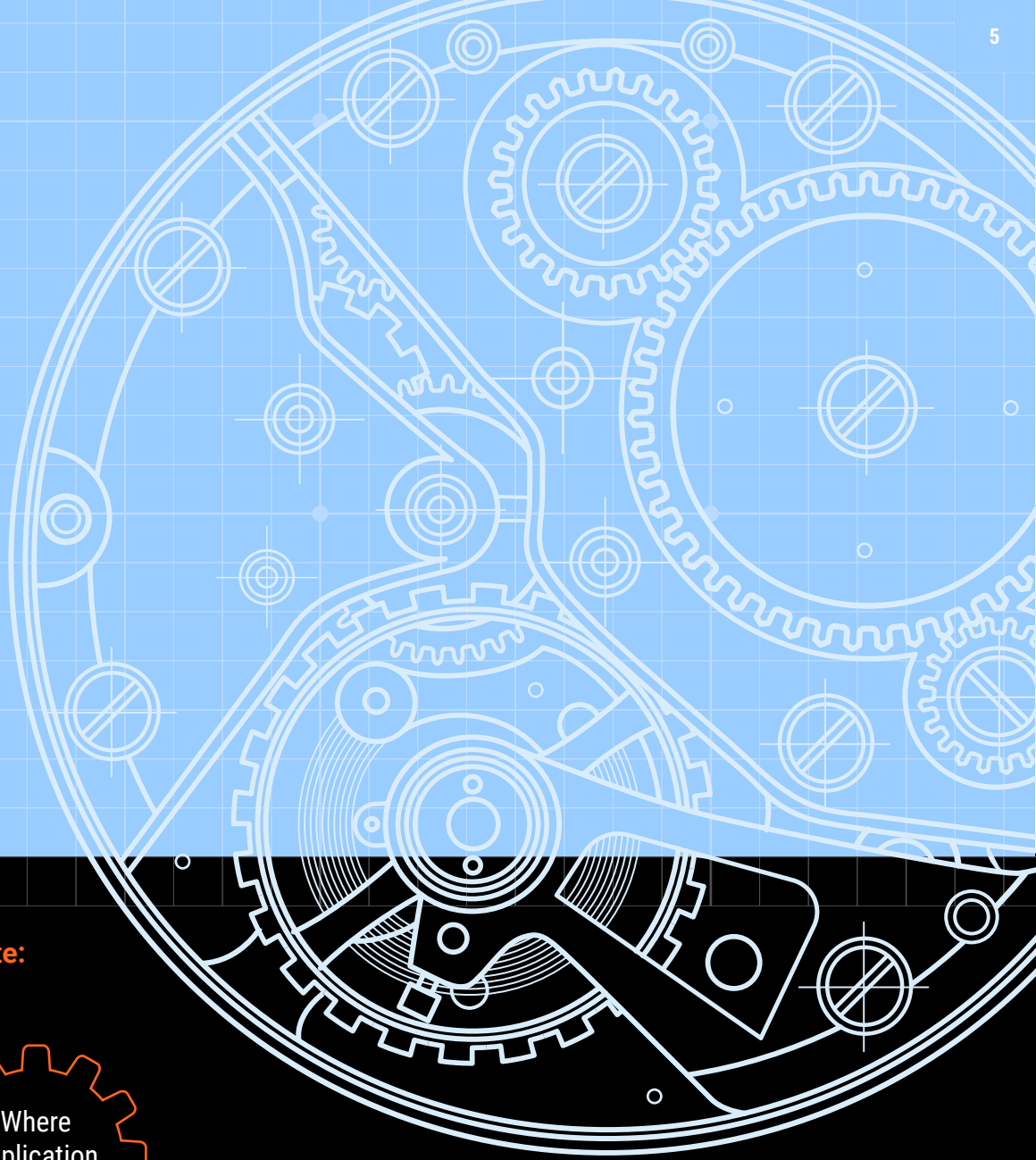
3 "IC3 2009 Annual Report on Internet Crime Released", FBI, March 12, 2010.

Discovering Cost Inefficiencies

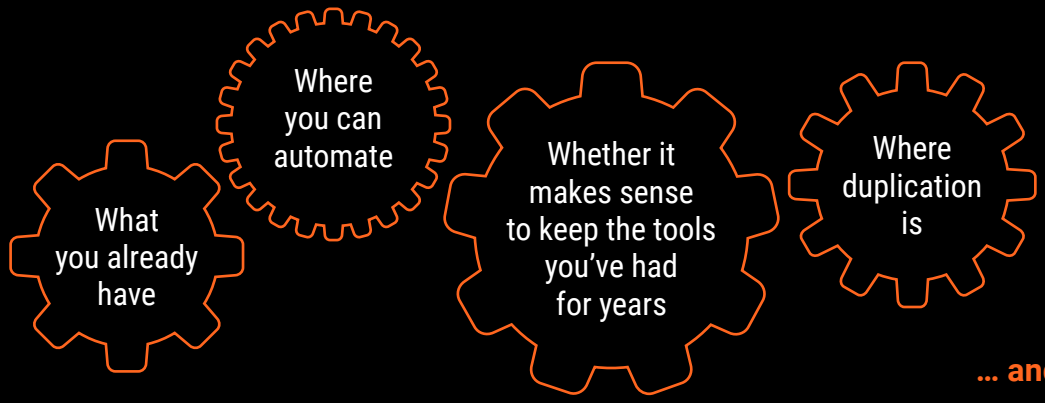
Time is crucial in cybersecurity. For every second an organization spends trying to find and contain a security breach, an attacker gains more time to create damage. Therefore, it's always in everyone's best interest to remediate an incident as fast as possible.

But you can't do that when your security team has to spend most of their time finding and gathering key information. Security analysts spend an average of five minutes[4] manually correlating disparate data sources just to obtain the right context before they can respond to an incident.

Freeing up your team from manual repetitive tasks not only allows them to speed up incident response, but it also gives them time to focus more on strategic initiatives and deliver ROI. And that's just one example of a cost inefficiency. Identifying others can help you re-evaluate.

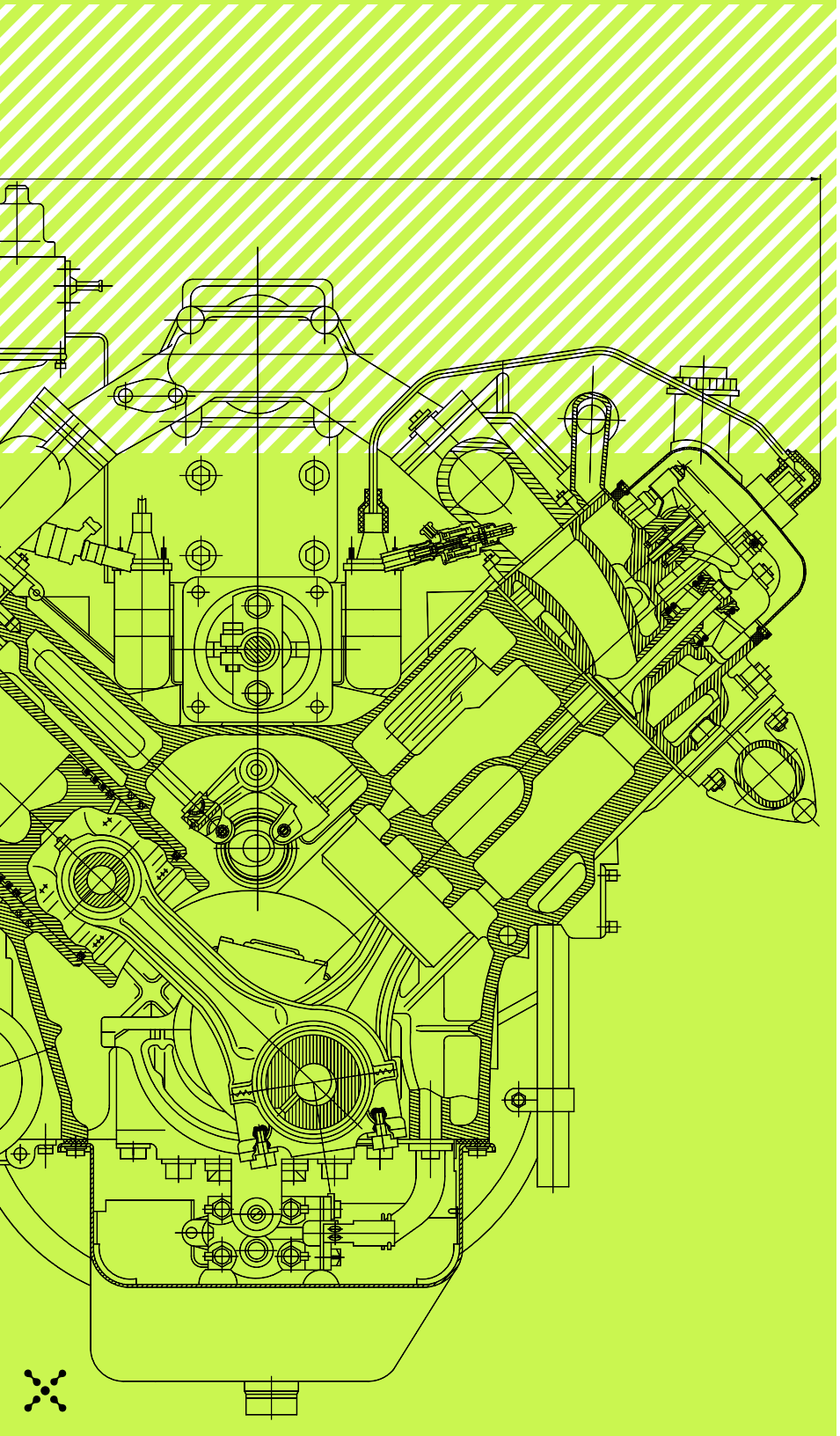


By looking closely at cost inefficiencies, you can re-evaluate:



… and so much more.

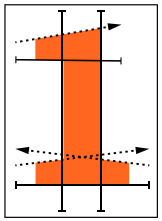
4 "Reducing Alert Triage Time in the Security Operations Center (SOC)", Patrick Kelley, Axonius, December 11, 2020.



The Role of Ownership in Cost Inefficiencies

Part of identifying cost inefficiencies means working with business owners and understanding what their priorities are. The business owner may need a certain tool or asset to achieve a goal or solve a pain point. Alternatively, you might discover technology once thought to be important to the business owner's objectives isn't actually necessary.

Ultimately, a conversation between IT, security, and business owners is necessary to determine whether the tools your organization has purchased are actually doing the job required of them — or if they're leading to unnecessary costs.

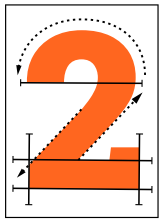


UNCOVERING INEFFICIENCIES FROM UNTAPPED INFRASTRUCTURE

One way to recover budget is by finding tools that aren't being used at all. Licensing is one area with *a lot* of potential for cost inefficiencies.

For example, it's often customary to send out the same software to every new employee — even if the software installed isn't always going to be used by each individual. Let's imagine 9,500 software licenses were purchased, but there are about 9,400 employees. That's at least 100 software licenses not in use — money left on the table.

Also consider when employees leave, and a company doesn't backfill that position. Those employees might still have access to company SaaS applications outside of their company's Single Sign-On. Or software remaining on their devices doesn't get transferred or removed, and those licenses remain active long after they've gone.

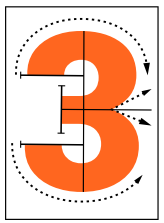


DISCOVERING INEFFICIENCIES FROM FORGOTTEN INFRASTRUCTURE

If you don't know what's being used, then you're potentially spending money on infrastructure that's no longer relevant.

Take virtual machines (VMs), for example. These are so easy to spin up that it's not unrealistic or unreasonable for an organization to have hundreds of thousands of VM instances. But many remain up and running long after their intended use is no longer relevant.

The cost of all those unused VMs can add up real fast.



IDENTIFYING INEFFICIENCIES IN OVERLAPPING INFRASTRUCTURE

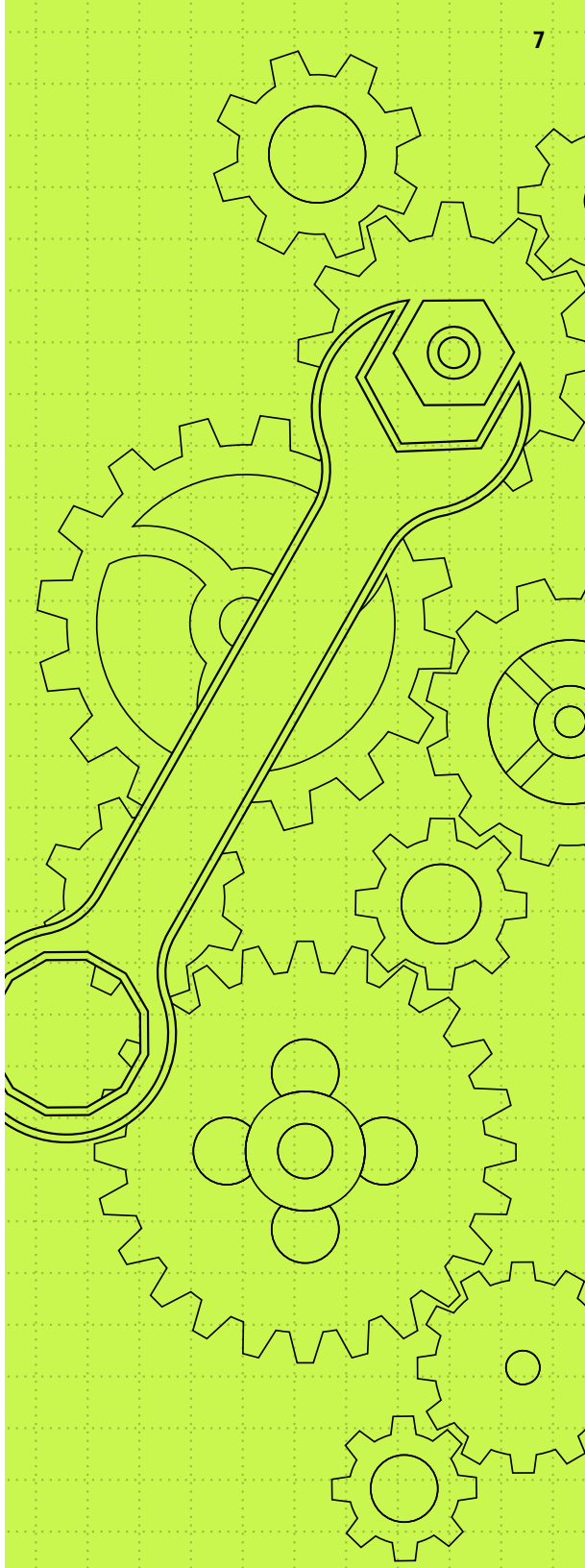
Organizations buy a variety of tools for all sorts of reasons. Inevitably, some of those tools are going to have overlapping features or functionality. (And this is definitely true if teams are working in silos or aren't regularly talking with each other.)

Let's say you have endpoint protection for Windows machines. But you have different versions: one each from Crowdstrike, Trend Micro, and Windows Defender.

So now you've got three tools all taking on the same task. Why?

Well, there are probably a lot of reasons. A tool may have been purchased for one purpose, but turns out there's more functionality than originally thought. Someone else may have bought a tool, but it was too hard to deploy. Maybe the third person had tons of budget and bought a bunch of tech that never got fully utilized.

While the logic for initially purchasing these three separate tools may pan out, keeping all of them does not. Determine what tool makes the most sense to keep and eliminate the others.

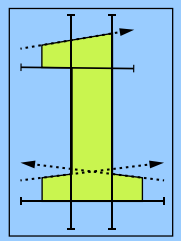


Resolving the Challenges of Cost Inefficiencies

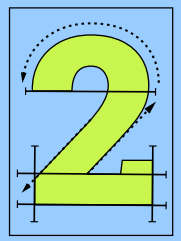
Once you've identified where the unrealized spend is, it's time to address it.

Collaboration is key. That means working with business owners to understand why a specific tool is necessary. By partnering with other departments, your team can find cost inefficiencies faster.

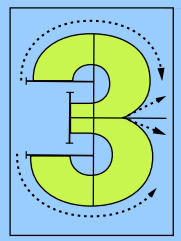
Here are four key ways to help everyone understand each other's needs:



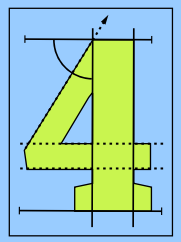
Establish an ongoing process to indicate what tools aren't being used or optimized as initially anticipated.



Analyze how an individual tool is broadly used across the organization.



Work with owners or administrators to understand the context and justification for the tool.



Automate where you can and think about both the hard and soft costs. The most meaningful asset to any organization is human capital and ensuring you're getting the most value out of your employees' skills and experience. That's definitely not going to happen if they're spending a bulk of their time on low-value manual processes.

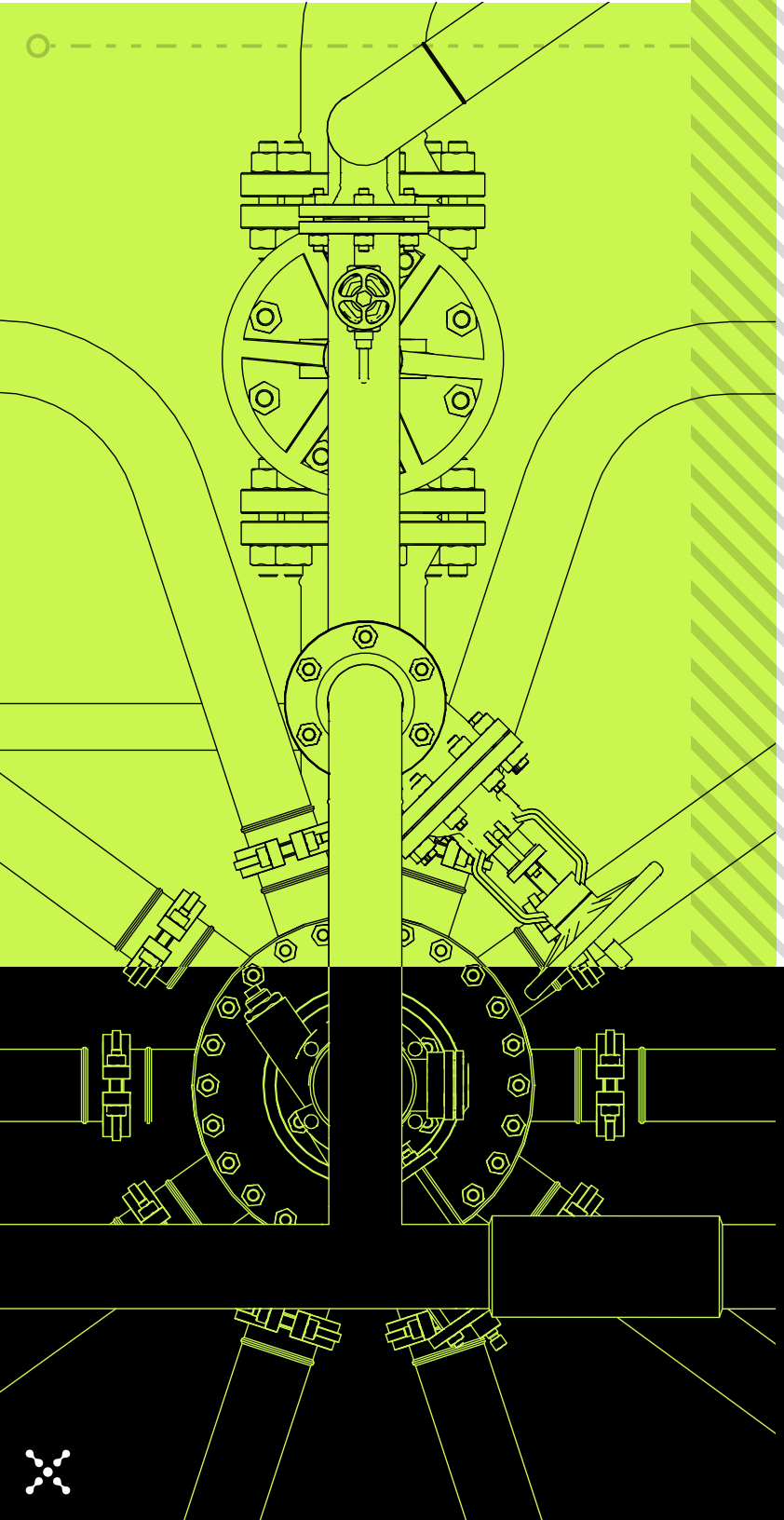
Measuring the Value of Cost Optimization

What does unrealized spend mean to you and your team?

Well, a lot.

Through optimizing hard costs, you'll find more budget savings and less money spent. That's a lot of cash you can reinvest into your team. And identifying areas where you can cut back on those hard costs will also help you better manage and justify the budget you do have.

When it comes to soft costs, it's really about people — your team. Looking for ways to work more efficiently keeps employees engaged and focused on your organization's strategic initiatives. By creating a fulfilling experience for your team, you're able to justify their roles and avoid layoffs.



How DCU Gained Visibility Into Efficiencies

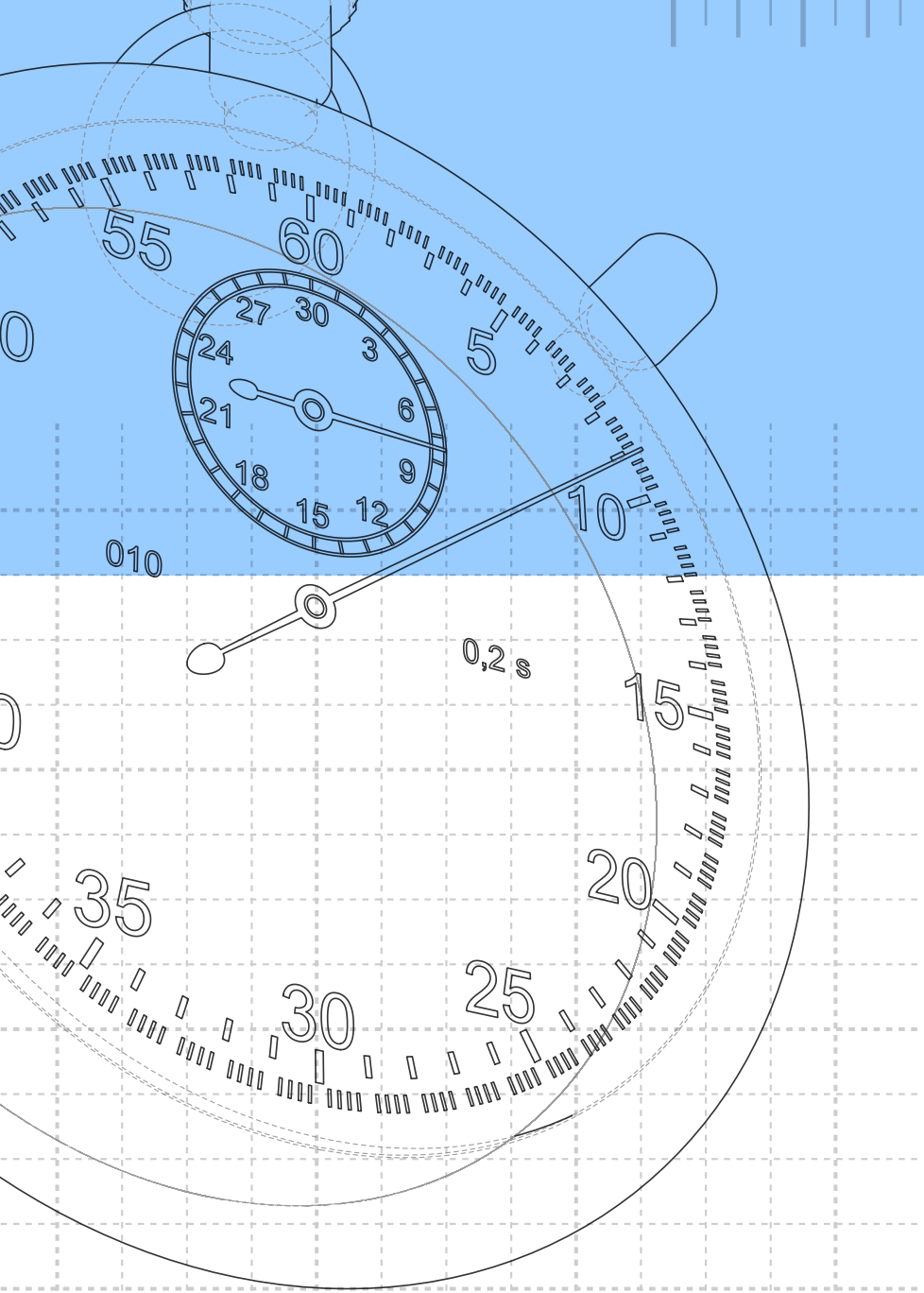
Network visibility can elude even the most dedicated cybersecurity teams. And that includes the team at Digital Federal Credit Union (DCU).

Understanding all of the company's systems proved to be slow and tedious. The DCU cybersecurity team had to comb through data from multiple (and often siloed) systems to try to put together an accurate security asset picture. But the team lacked insight into its environment and struggled to discover unprotected assets.

Through Axonius, the DCU team integrated their IT and security systems to view them in one central, searchable console. They gained unprecedented visibility and understanding of their entire asset inventory, coverage gaps, and more.

> **If you don't have something pulling that all together for you, the best you can do is work with spreadsheets to pull all this data manually out of all the different systems. It would take you a month just to reconcile all that. [Axonius] does it for you every single night.**
>
> *— Mike Conroy, assistant manager of information security risk management, DCU*

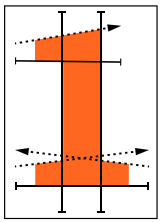
MAKING THE MOST OF WHAT YOU HAVE



3 Ways to Find Cost Inefficiencies

There are lots of actions you can take to identify unrealized spend and optimize costs. But actually doing so is easier said than done.

The good news? Following these three steps can get you there a whole lot faster.



FREE UP YOUR SCARCEST RESOURCE

Time is the one thing we don't ever have enough of — and we can't buy more. Your team is already jam-packed 24/7, and taking time to manually track down assets prevents them from tackling more strategic tasks.

So find opportunities for automation.

Look at vulnerability management, for example. Manually identifying and prioritizing vulnerabilities, validating vulnerability security policies, and confirming successful outcomes can pose challenges without automation. Especially when you need to connect vulnerabilities to specific devices and software.

Luckily, there are tools available to automate the whole process. In return, your team can now pivot from chasing down asset data to focusing on more strategic initiatives that drive your function and the business forward.

2. ENSURE INFRASTRUCTURE IS SUFFICIENTLY DEPLOYED

Imagine overseeing an organization with multiple business units — all of which are highly decentralized. Each unit has their own separate set of systems and tools, causing challenges in managing and securing assets.

That's exactly the situation commerce company Cimpress was up against before it sought out a cybersecurity asset attack surface management (CAASM) solution.

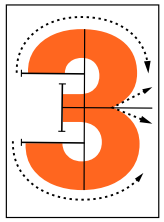
The company invests in and operates a wide variety of businesses that use mass customization to configure and produce small quantities of individually customized goods across the globe.

But with over 12,000 employees and 11 distinct businesses operating underneath its umbrella, the company's Manager of Security Engineering Daniel Fabbo soon found himself having to connect disparate infrastructures each with their own rudimentary asset management system.

As a result, Fabbo and his team found it difficult to identify gaps in the company's antivirus and EDR coverage. And when the security team identified an incident or vulnerability, it was nearly impossible to locate and then understand the particular asset or assets in question.

Axonius managed to help Cimpress gain visibility into each of its separate businesses' systems and tools, discover coverage gaps, and help keep a clean, up-to-date asset inventory.

> **Prior to using Axonius, we had about 40% coverage of our EDR deployment. And after Axonius, we were able to identify those areas where we were missing coverage and were able to increase that to 80%.**
>
> *— Daniel Fabbo, Manager of Security Engineering, Cimpress*



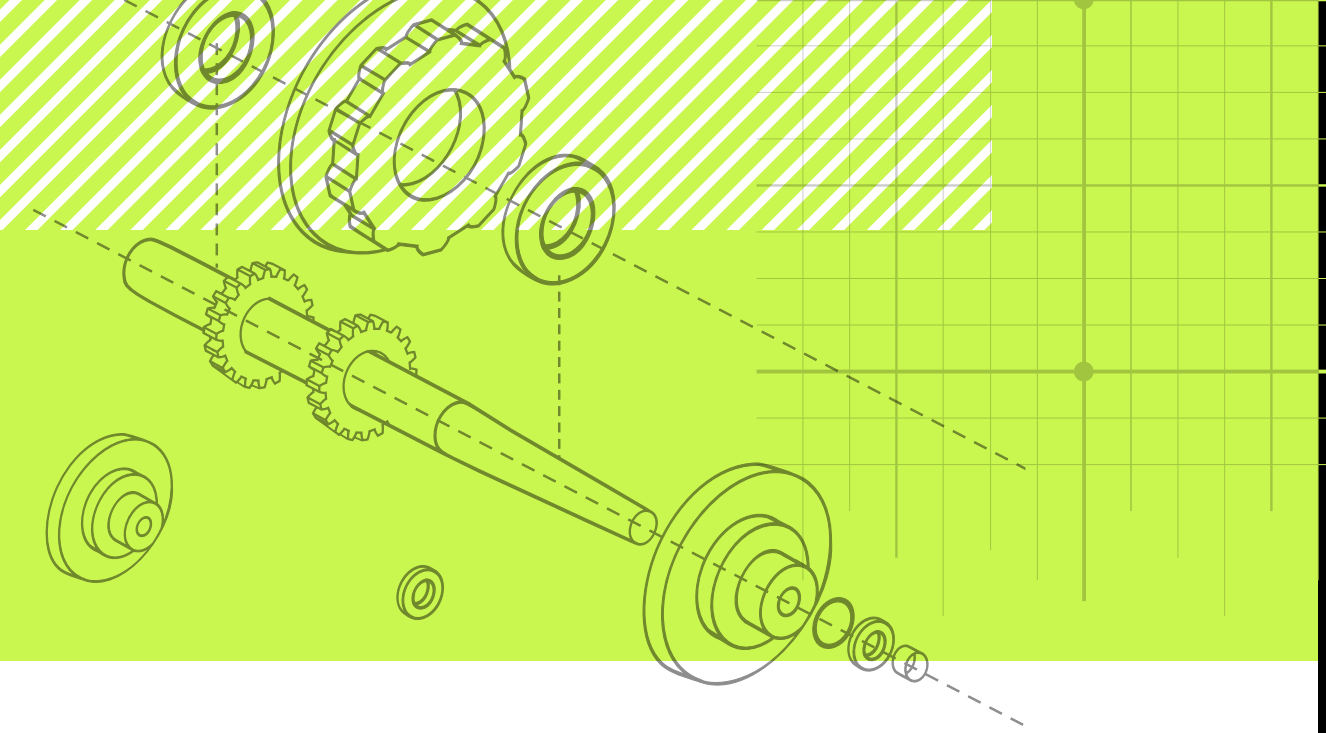
JUSTIFY THE VALUE OF NEW AND CURRENT INFRASTRUCTURE

Over the last 10 years, the usage and demand for SaaS applications have exploded. More recently, SaaS apps became the go-to solution for helping companies transition to remote work during the pandemic.

But the shift to SaaS only increased the challenges for IT and security teams. It's no longer easy to know all the SaaS applications an organization has. But it's all too easy for individual teams to purchase and download SaaS apps each day.

Take sales and marketing, who are heavy users of SaaS. It's highly likely both departments could benefit from the same SaaS applications to target accounts, communicate with customers, and expand outreach. But they're probably not talking to each other, and instead are using two different SaaS applications for the same actions.

Getting deeper visibility into all the SaaS apps in use can also provide visibility into spend — specifically, whether there are redundant apps, or underused or duplicate SaaS licenses.



How Plansource Identified Cost Efficiencies

For HR tech organization PlanSource, knowing what assets are in their environment — and what the possible vulnerabilities in that environment may be — is at the core of protecting sensitive and private employee data. Yet the company struggled with understanding what inventory they had and instead were left with gaps in detecting and remediating vulnerabilities.

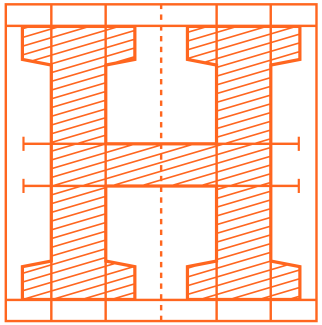
PLANSOURCE

Multiple teams would come up with different answers for what assets were on the company's network, making it difficult to understand the true state of their IT environment. Their current inventorying processes were also time consuming and disruptive.

But Axonius enabled PlanSource to automate areas that they weren't able to before, giving the company a level of unmatched visibility. As a result, PlanSource's IT and security teams saved person-hours and gained a more accurate understanding of what's happening in their environment.

> **We can automate more tasks because we have a source of truth that can tell us if something's net-new, if something's out of compliance, if something's in a state that's not what we consider normal. Before that, it would've taken a lot of [person]-hours to get to that point.**
>
> *— David Christensen, VP and CISO, PlanSource*

THE ROI OF COST OPTIMIZATION



ow do you know whether or not cost optimization is worth the effort?

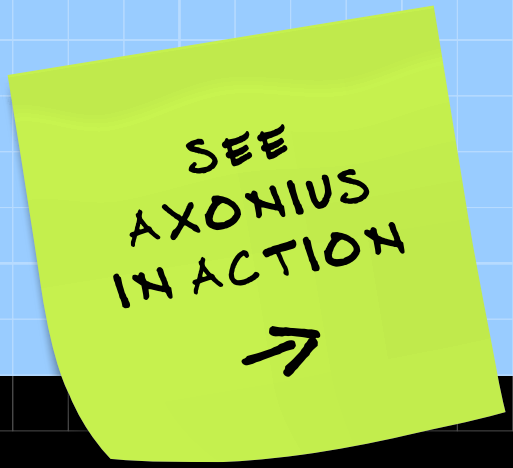
You have to calculate the return on investment.

Look at how many hours a month you have your people spending on things like uncovering broken or missing controls. Calculate what you're spending on software licenses that aren't being used and compare that with your budget.

Identifying ROI can help you better understand the state of spend in your organization. For example, there may be spend that can be recovered in terms of automation and eliminating misused or unused tools. By eliminating it, you can then justify things like keeping your team or pushing forward new initiatives initially paused due to budget constraints.

With IT budgets under closer scrutiny than ever before, C-suite leaders are looking for ways to boost their business advantage. And by identifying inefficient spend and its ROI, you can not only put dollars back into the business, but also into your team.

See how you can **identify** unrealized spend, show **ROI**, and deliver **cost optimization** while continuing to **protect** your attack surface with **Axonius**.



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.

AXONIUS

Axonius.com