BUILDING THE BUSINESS CASE FOR A **CYBERSECURITY ASSET MANAGEMENT SOLUTION**

AXONIUS

MODERN BUSINESSES **ARE EVOLVING AT A BREAKNECK PACE.**

As more organizations pivot to digital-first, their IT and security teams are poised to play a more strategic role — one that moves beyond support to effectively scale and secure their business.

Continuous visibility into today's complex IT infrastructure — beginning with an accurate asset inventory of devices, applications, and users — is foundational to this effort.

And with all of the great IT and security tools businesses have today, shouldn't that be easy?

The truth is, many asset management tools offer individual pieces of the asset puzzle. *The result?* The information needed about assets lives in different silos, making it hard to ask asset-related questions, get answers, and take action.

Here's the good news: All the data you need already exists — and the solutions that know about your assets have APIs. All you need is a way to collect, correlate, and take action.

That's exactly where a cybersecurity asset management solution comes in handy. *How?* It helps IT and security teams implement an approach that automatically and continuously discovers assets in their environment — and provides a single source of truth into all assets.

IT and security teams understand that. But how do they make the business case for implementation of a cybersecurity asset management platform?

> **YOU CAN HAVE A LOT OF DISPARATE SYSTEMS MANAGED BY DISPARATE TEAMS, AND IT CAN BE HARD TO GAIN A COMPREHENSIVE VIEW OF WHAT'S ON YOUR NETWORK.**
>
> ***– Jason Loomis, CISO, Mindbody***

READ ON TO EXPLORE KEY POINTS TO HIGHLIGHT WHEN MAKING A SOLID BUSINESS CASE, INCLUDING:

- **The myriad business functions that can benefit from comprehensive asset management**
- **Cost and time savings that cybersecurity asset management can bring**
- **Key use cases that the Axonius Cybersecurity Asset Management Platform helps with**

72%

Organizations reporting increased IT complexity in the past two years

Many organizations report widening visibility gaps in their

79% **Cloud Infrastructure**

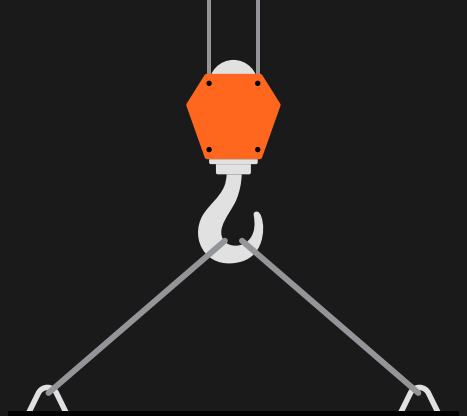
75% **End-user Devices**

75% **IoT Devices**

82%

Organizations planning to increase asset inventory investment

Source: *"Cybersecurity Asset Management Trends 2021: How the Rapid Shift to Remote Work Impacted IT Complexity and Post-Pandemic Security Priorities." ESG and Axonius. 2021.*



SECTION

1

WHAT DOES **COMPREHENSIVE ASSET MANAGEMENT DELIVER?**

> **SIMPLY PUT, IF YOU DON'T KNOW ABOUT AN ASSET, YOU CAN'T PROTECT IT.**
>
> *– Doug Graham, Chief Trust Officer, Lionbridge*

Gone are the days when asset management was just an IT problem. Today, a comprehensive asset management program is foundational to an array of IT and security initiatives. It's integral to improving your organization's security posture.

But as assets become highly distributed, they're becoming harder to manage and inventory.

A modern cybersecurity asset management platform integrates with existing security and management tools to gather asset details from a variety of data sources. This creates a complete inventory of all assets — whether managed or unmanaged, in the cloud or on premises. Plus, these tools help discover security solution coverage gaps and automate security policy enforcement.

When making a business case for cybersecurity asset management, there are many areas IT and security leaders can highlight that go beyond traditional asset management.

LET'S TAKE A LOOK AT A FEW.

SECURITY OPERATIONS AND INCIDENT RESPONSE

Security analysts spend loads of time correlating alert data with asset data to try and effectively triage alerts. Without a single view into all assets, security operations teams need to cross reference several tools and make assumptions. *The result?* Delays in alert triage and incident resolution.

An up-to-date, comprehensive asset inventory helps security analysts correlate alerts, understand the relationship between devices and users, and look at the current and historical state of an IT asset. It helps them quickly gather the context and detail needed to inform their investigations, accelerating the overall process.

$4.24M:
Cost of a data breach

128 DAYS:
Average time to detect and contain a data breach

Source: *"Cost of a Data Breach Report 2021." Ponemon Institute and IBM. 2021.*

VULNERABILITY MANAGEMENT

An important aspect of securing modern businesses is the ability to rapidly identify the presence of vulnerabilities across all asset types. But with new security vulnerabilities emerging every day, there's an endless backlog of vulnerabilities for teams to deal with.

Increase in device diversity — coupled with finding devices that already have outdated and vulnerable software — pose another challenge for security and IT teams. Prioritization is critical, but it's hard to prioritize if you don't understand your assets and how they're configured.

Gathering asset data to optimize vulnerability and patch management initiatives is a manual, time-consuming task that can ultimately lead to a loss in visibility and increased risk.

Cybersecurity asset management solutions integrate with leading vulnerability management platforms to provide a correlated view of vulnerabilities and severity levels for each. IT and security teams can then trigger automated action to mitigate the risk from security vulnerabilities.

50 **Number of new CVEs logged *each* day**

Source: *Redscan analysis of NIST and National Vulnerability Database*

GRC AND AUDIT

One of the most common challenges when dealing with asset management for compliance and audits is accurately tracking and accounting for all in-scope assets in their environment. *The implication?* Opening organizations to risks and consequences of non-compliance.

Security, IT, and risk teams also spend hours each quarter preparing asset inventories for internal and external audits.

A cybersecurity asset management platform can continuously gather an inventory of all in-scope assets and help you understand the configuration of each asset. This allows GRC teams to streamline the process, continuously monitor risks presented from IT assets, and identify the results of compliance initiatives such as HIPAA and NIST.

Average revenue losses for businesses due to non-compliance

Source: *"The True Cost of Compliance with Data Protection Regulations." Globalscape and Ponemon Institute.*

IT OPERATIONS

ITOps plays a critical role in accomplishing business goals. Among other things, these teams help maintain a reliable IT ecosystem, provide secure remote access to authorized users, and ensure that IT enables the organization to achieve the desired business outcomes.

To do all this, they need full visibility into their environment — beginning with an accurate inventory of all devices and workloads. But traditional asset inventory approaches are manual, time-consuming, fragmented, and practically impossible to keep up to date.

A cybersecurity asset management platform helps ITOps teams by automatically gathering asset inventory, applying and verifying risk controls, and mapping asset inventories to compliance frameworks.

76% **IT pros who believe IT complexity is the biggest barrier to productivity among ITOPs teams**

61% **believe reliance on manual processes is another productivity barrier**

Source: *"The Impact of Automation on IT Operations." Freeform Dynamics and Fujitsu.*

CLOUD SECURITY AND CONFIGURATION

Misconfigurations are one of the most common ways cybercriminals gain a foothold in your cloud environment, assault company networks, and initiate cloud-jacking.

To ensure all public cloud workloads are properly configured, security and IT teams must continuously monitor changes to configuration details — and understand the context and risk of any change at scale. But their ephemeral and elastic nature makes this an uphill battle.

A cybersecurity asset management platform delivers complete visibility across all cloud assets by unifying cloud asset data from multiple providers. It helps discover cloud instances that aren't being protected and/or are publicly accessible, driving visibility while slashing the manual labor needed to obtain an aggregate view.

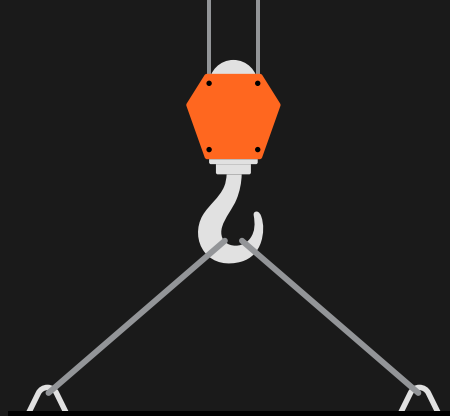
In fact, organizations that don't have visibility gaps report a 70% reduction in public cloud security incidents compared to organizations that do have gaps.[1]

8/10

Companies across the U.S. that have experienced a data breach made possible by cloud misconfigurations

Source: *"Risk Of Cloud Access Permissions." IDC. 2020.*

[1] *"Cybersecurity Asset Management Trends 2021: How the Rapid Shift to Remote Work Impacted IT Complexity and Post-Pandemic Security Priorities." ESG and Axonius. 2021.*



SECTION

2

MAKING THE **BUSINESS CASE**

THERE'S NO DENYING THE FACT THAT MOST IT AND SECURITY TEAMS ARE OVERWORKED — AND UNDERSTAFFED.

And there's a clear risk there. The more overworked IT and security teams are, the harder it is for them to spot and respond to real threats.

Let's look at how deploying a cybersecurity asset management solution can cut costs and help the business.

83% **of cybersecurity professionals feel overworked**

82% **of security teams are understaffed**

Source: *"Cybersecurity Skills Gap Report 2020." Tripwire.*

TIME REDUCTION

Sixty-four percent of organizations approach asset inventory as a monthly or quarterly event.[2] This cadence leaves significant visibility gaps in between, resulting in unmeasurable business risk and taking away from other high-priority tasks.

Automating cybersecurity asset management results in significant time reduction for gaining a complete asset inventory — accelerating incident response, finding and patching critical vulnerabilities, security policy validation and enforcement, and more.

How does it help the business? With time reduction on asset related tasks, businesses can refocus IT and security talent toward higher-value tasks including:

- **Deploying new IT and security technologies and processes**
- **Implementing a proactive approach to security by implementing threat hunting**
- **Responding to high-priority incidents and attacks**

86 **Hours of labor needed to compile a manual asset inventory**

8 **Average number of tools used for asset inventory**

Source: *Cybersecurity Asset Management Trends 2021: How the Rapid Shift to Remote Work Impacted IT Complexity and Post-Pandemic Security Priorities*

[2] *"Cybersecurity Asset Management Trends 2021: How the Rapid Shift to Remote Work Impacted IT Complexity and Post-Pandemic Security Priorities." ESG and Axonius. 2021.*

ENSURING FULL DEPLOYMENT OF PURCHASED SOLUTION

Often, technologies are purchased but either aren't fully deployed or aren't used right away. It's time-consuming and manual to identify devices missing security controls like encryption, endpoint security agents, vulnerability scans, and more.

The result? Businesses are likely losing value and/or overpaying for software purchases. Comprehensive asset management can see if a new technology is up and running, how often it's being used, how often it's accessed, and by whom.

A cybersecurity asset management platform can also automatically discover devices missing security controls. This eliminates manual correlation of disparate data sources and reduces the time needed to accomplish the task.

RISK REDUCTION

Given the ever-expanding threat landscape, risk reduction is imperative for business success.

Let's look at some easily identifiable areas of risk reduction that can be achieved with cybersecurity asset management:

- **Getting a comprehensive and always up-to-date inventory of all assets will *increase visibility and ultimately reduce the likelihood of incidents occurring***
- **Ensuring wide deployment of security technologies (encryption, EDR, EPP, vulnerability management) can *minimize the impact of incidents***
- **Having contextualized, historical asset data reduces the time needed to investigate alerts and *improves the mean time to recovery metric***
- **Continuous validation of every asset's adherence to the overall security policy and automating response actions whenever a user or device deviates from policies help improve overall security posture**

$10.5T:

Estimated annual cost of cybercrime by 2025

Source: *Cybersecurity Ventures. 2020.*

SECTION

3

DEEP DIVE: ASSET MANAGEMENT SAVINGS

Without an accurate understanding of everything in your environment, all other initiatives suffer. But security and IT teams lose valuable time and resources when spending time creating credible, comprehensive asset inventories and tracking down necessary asset data.

BY LEVERAGING CYBERSECURITY ASSET MANAGEMENT PLATFORMS, ORGANIZATIONS ELIMINATE THE MANUAL WORK IT AND SECURITY TEAMS SPEND ON BASIC ASSET MANAGEMENT.

TIME TO GATHER ASSET DATA

A cybersecurity asset management platform saves costs in full-time equivalent (FTE) time by automatically aggregating, normalizing, and correlating asset data to deliver a comprehensive asset inventory. Getting a complete asset inventory is attainable in hours, saving organizations an average of 86 person-hours of labor many times per year[3].

Given that data source diversity is key in gaining a comprehensive asset inventory, these platforms are designed to ingest data from multiple data sources (through API integrations). The result? IT and security teams get a detailed look into each asset, including installed software and agent versions, hard drive capacity and utilization, operating system versions, and more.

Armed with this data, it takes only seconds to gather a list of assets that have common IT and security risks, like:

- **Legacy technology: Machines running unsupported operating systems**
- **Availability risk: Whether certain assets have experienced significant downtime**
- **Security vulnerabilities and IT hygiene: Understand if machines are running outdated software, and if users are properly using IAM solutions**

[3]"Cybersecurity Asset Management Trends 2021: How the Rapid Shift to Remote Work Impacted IT Complexity and Post-Pandemic Security Priorities." ESG and Axonius. 2021.

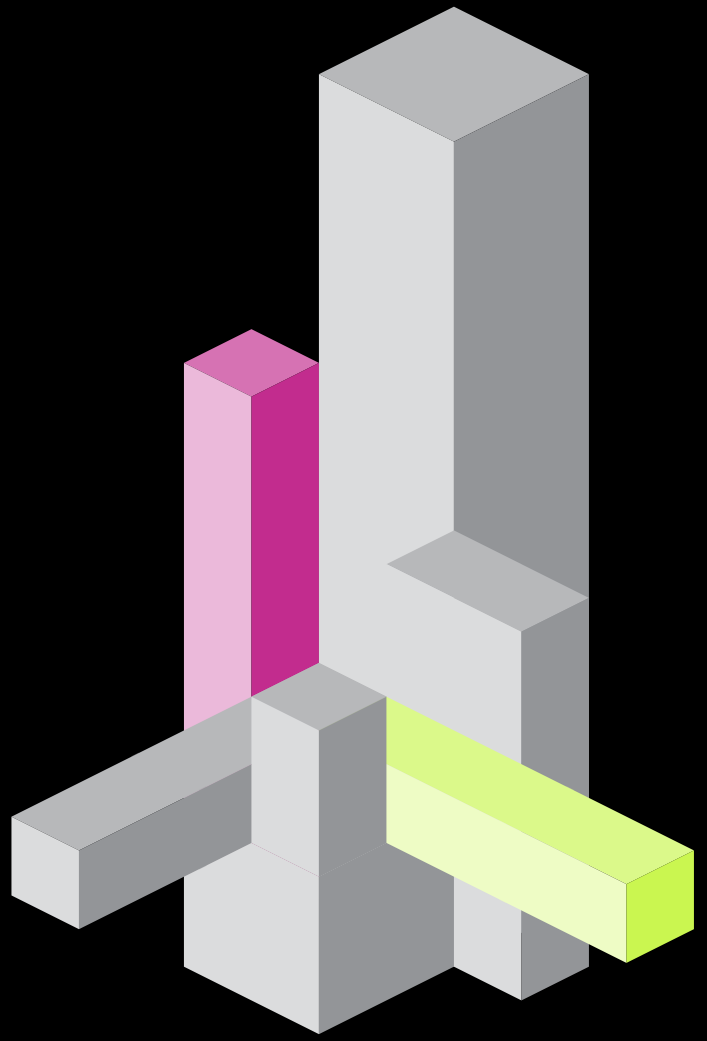
TIME SPENT MAINTAINING CMDBS

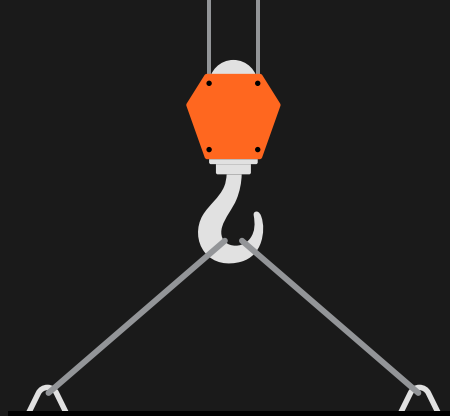
CMDBs are great at storing information about asset configuration, but IT and security teams spend countless hours, dollars, and effort in initial setup (making the time-to-value suffer greatly) and customization.

But CMDBs often lack the data truly needed to understand an asset. And with data structures changing over time, it makes it difficult and expensive to constantly update CMDB tools to collect the right data.

Another CMDB challenge? They're often problematic because of data conflicts — data inputs into CMDBs typically have a wide variety in naming conventions, and even fields like OS type, OS version, full OS string, host name, and others vary frequently.

A cybersecurity asset management platform aggregates and deconflicts asset data to provide a singular, credible view into any asset. Once all assets are seen in the platform, security and IT teams can find gaps and discrepancies present. It also helps enrich existing CMDB entries.





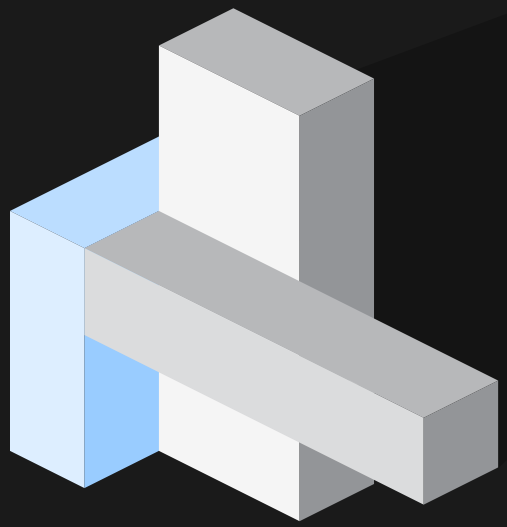
SECTION

4

HOW **AXONIUS CAN HELP** REIN IN COMPLEXITY

The Axonius platform gives our customers a way to manage cyber risk by enumerating extensive traits and characteristics about each asset — no matter who, what, or where.

Let's delve into a few important use cases to see how Axonius can help empower IT and security teams.



USE CASE: **VULNERABILITY MANAGEMENT**

Today's vulnerability assessment tools do an incredible job of identifying known vulnerabilities present on the *devices they're aware of*. But how can we ensure that all assets — including virtual machines and cloud instances — are being scanned?

While accessing the admin console of a VA scanner in use offers a list of covered devices, the problem lies in knowing *which devices should be scanned but aren't part of the VA scan schedule*.

Axonius helps aggregate and correlate data from multiple sources (VA scanner console, network, IAM solutions, and cloud infrastructure) to understand which of your devices, cloud instances, and virtual machines aren't part of the VA scan schedule.

Plus, Axonius can be used to group systems by a wide variety of characteristics — including subnet, VLAN, operating system, ownership, and more — to prioritize vulnerability management and patching.

By running simple queries in the Axonius Query Wizard, IT and security teams can identify all devices running applications that may be affected by vulnerabilities. What's more, the Axonius Security Policy Enforcement Center lets them trigger automated action. For instance, users can create an incident and alert asset owners so they can take immediate action to patch.

> **AXONIUS HAS GIVEN US VISIBILITY THAT PREVIOUSLY WOULD HAVE REQUIRED US TO TAKE MULTIPLE OUTPUTS FROM DIFFERENT SOURCES AND CORRELATE THEM TO GLEAN A RESULT. AXONIUS GREATLY REDUCED THE TIME WE WOULD HAVE SPENT, AND INCREASED OUR ACCURACY.**
>
> ***– Steve Kjaer, CISO, Poly***

For more information, read Finding Devices Not Being Scanned For Vulnerabilities.

USE CASE: **SECURITY SOLUTION DEPLOYMENT**

Organizations spend significantly on security tools — only to later realize these tools aren't deployed everywhere they should be. Axonius helps recoup lost value by continuously surfacing assets missing agents and software deployments. This helps protect the entire attack surface — and ensures that when devices without agents are discovered, you can automatically inform the right team.

A common use case for Axonius customers? Finding devices that are missing specific endpoint agents. Agents generally run continuously and silently in the background, gathering data about the state of the device. Accessing the admin console of the agent produces a list of covered devices. *The real challenge?* Uncovering devices that should have the recommended agent, but don't.

Using the Query Wizard, Axonius customers can find devices missing an endpoint agent. Queries can be as simple as looking at any identified asset that doesn't have any agent installed whatsoever and is only known to the network, or detailed queries to find devices by OS type that are missing the requisite EDR and EPP solution.

For more information, read Finding Assets Missing Endpoints Agents.

Axonius can also help find devices with malfunctioning agents.

> **OUR SECURITY AGENT DEPLOYMENT RATE HAS SHOTUP PRETTY DRAMATICALLY. WE WENT FROM 60% AND 70% ON SOME AGENTS TO ABOVE 95% WITHIN ABOUT A FOUR-MONTH PERIOD — PRETTY DRAMATIC RESULTS GIVEN THE NUMBER OF DEVICES THAT WE HAVE.**
>
> ***– Greg Thomas, security analyst II, Trexis Insurance***

USE CASE: **ACCELERATE INCIDENT RESPONSE INVESTIGATIONS**

Finding devices that may be associated with an incident can be a daunting task. *Why?* Security analysts often receive alerts that tell them what happened and how, but are then forced to spend time tracking associated devices.

Axonius gives you a single source of truth into assets to speed alert triage, and allows you to view historical data to match asset attributes with the time of the indicator of compromise.

By connecting adapter sources that provide rich information on devices, users, and cloud assets, security analysts can easily correlate alerts with data in Axonius to answer critical incident response questions, like:

- **Which devices and users were associated with the alerts?**
- **Where are the devices located and what software is running on the device?**

A simple but effective way to speed up incident investigations is to query Axonius for any IP address provided in alerts. Security analysts can then trigger enforcement actions, including notifying teams, or isolating incidents by taking actions on devices and users directly.

> **AXONIUS REALLY ENABLED US TO CONDUCT A FULLY ROBUST INVESTIGATION, QUITE LITERALLY IN ONE PLACE. IT'S INCREDIBLY EASY TO BUILD A USER PROFILE WHEN AN INVESTIGATION COMES UP — AND THAT MEANS INVESTIGATION ACROSS ANY BOARD, WHETHER THAT BE INCIDENT RESPONSE OR VULNERABILITY MANAGEMENT. I THINK THAT VERY FEW SOLUTIONS ARE ABLE TO PROVIDE SOMETHING LIKE THAT.**
>
> ***– Andrea Youwakim, security analyst, Avant***

For more information, read Accelerating Incident Response Investigations With Axonius.

USE CASE: CLOUD SECURITY AND CONFIGURATION

Cloud adoption has long become mainstream. However, cloud misconfigurations, overly permissive access rights, and publicly available data means many organizations still struggle to secure all cloud instances.

To identify cloud instances not being scanned for vulnerabilities with Axonius, there are simple queries you can build — ranging from the broadest possible scenario to the most detailed. A basic query might be finding AWS instances not being scanned for vulnerabilities. Organizations can also filter the results further to show only AWS instances that have known CVEs and aren't being scanned for vulnerabilities, or only those instances that have a CVE severity of critical by changing the query.

And like with all other use cases, the Axonius Security Policy Enforcement Center allows customers to determine which automated action to execute when a cloud instance is found that's not being scanned.

For more information, read Discovering Cloud Instances Not Being Scanned for Vulnerabilities.

Now let's look at misconfigured cloud workloads or those not adhering to best practices. Misconfigured cloud workloads are those that fall short of guidelines listed by frameworks like the CIS Foundations Benchmarks.

Axonius Cloud Asset Compliance, an add-on to the Axonius platform, helps you see accounts or instances that adhere to or deviate from mandated policies. How? It uses cloud configuration and asset data from cloud IAAS providers and compares those implementations against industry benchmarks and frameworks.

For more detailed information, read Cloud Asset Compliance Overview.

USE CASE: EMPOWERING ITOPS TEAMS

Finally, let's look at a few ways Axonius can help ITOps teams:

- **Axonius continuously surfaces conditions in near-real time across the IT environment by connecting to all your data sources and taking historical snapshots of data. This provides a detailed view of how your IT environment has changed over time.**
- **Axonius helps increase the utility of CMDBs by speeding up the population of CMDBs with fully correlated asset data that doesn't require manual effort and time.**
- **Without having the right data all in one place, ensuring proper configuration of Windows and Linux servers is a challenge. Axonius details server configuration to ensure servers are up-to-date and covered by necessary security controls.**
- **Axonius aggregates data across IAM, directory services, and remote work and conferencing tools to monitor user access and changes in permission levels.**

> **AXONIUS HAS REDUCED THE TIME IT TAKES TO FIND ASSET INFORMATION FROM WHAT USED TO SOMETIMES BE 30 TO 60 MINUTES TO UNDER 30 SECONDS. IT HAS BEEN A HUGE EFFICIENCY WIN. IT ALSO SHINES LIGHT ON DARK PLACES IN THE ENVIRONMENT WHERE ASSET REPOSITORIES MAY HAVE GOTTEN CLUTTERED AND WHERE ASSETS MAY BE MISSING A BULK OF THE TOOLING YOU'D EXPECT TO SEE.**
>
> – *Gartner Peer Review*

SECTION

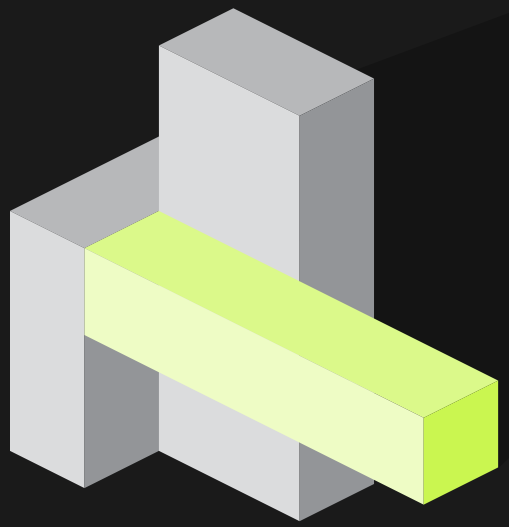
5

HARD SAVINGS: LET'S DO SOME MATH

What makes your business case stronger? Showcasing cost savings — and we're here to help.

Use our value calculator to see how Axonius saves time and allows you to reallocate resources. You'll get a customized report and analysis of the potential cost and time savings you'll receive with the Axonius platform.

Let's explore time and cost savings in alert triage and incident response, and vulnerability management.



ALERT TRIAGE AND INCIDENT RESPONSE

If you have a team that processes 200 alerts per month, and Axonius reduces the time needed to triage an alert by 90%, you can gain roughly $119,423 in savings, assuming:

- **40-hour work weeks or 2,080 working hours annually**
- **An average salary for an incident responder of $115,000**

		CURRENT	IMPACT	PROPOSED
C	Number of hours spent triaging alerts (monthly)	200	-90.0%	20
A	SOC / IR Specialist Salary	$115,000		$115,000
	Annual Total (c*12/2080*a), without realization	**$132,692**	**$119,423**	**$13,269**

Of course, the hours reduced on this task won't necessarily mean you no longer need full-time employees. Instead, it means your business can reallocate those employees' time to other high value initiatives.

AXONIUS.COM

See how you can calculate potential time and cost savings with the Axonius Cybersecurity Asset Management Platform.

SEE IT FOR YOURSELF

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

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with over 300 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.