EBOOK

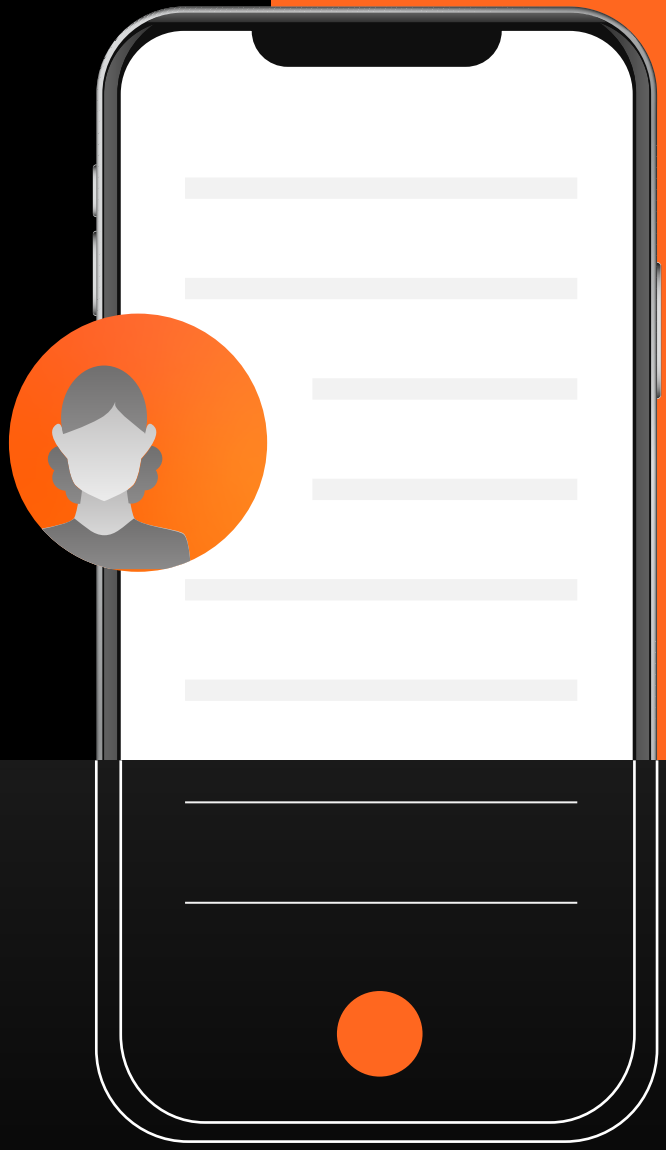
IN THEIR OWN WORDS:

WHAT SECURITY & IT TEAMS ACHIEVE WITH AUTOMATED ASSET MANAGEMENT

AXONIUS

WHEN ASKED, "HOW MANY DEVICES DO YOU HAVE?"

CISOs AND CIOs TYPICALLY RESPOND:



I don't know.

Between ***80*** and ***80,000.***

Even with it being the most critical foundation of cybersecurity, ***asset management is still a challenge.***

Is ***my agent*** **everywhere it should be?** ?

What ***unmanaged devices*** **are connected to privileged networks?** ?

Are your ***cloud instances*** **covered?** ?

These are the questions we want quick answers to, and yet so often find ourselves struggling to answer them.

Asset management is foundational to cybersecurity. Without an accurate understanding of everything in your environment, all other initiatives suffer. But traditional approaches to compiling an asset inventory are manual and error-prone. They're time consuming – and as soon as you have one, it quickly becomes obsolete.

The good news? It doesn't have to be this way. Cybersecurity asset management platforms give security teams unprecedented visibility by showing you all the assets in your environment, and then help you validate compliance and automate remediation.

>>> BUT DON'T JUST TAKE OUR WORD FOR IT.

Read on to see how Axonius customers have ***solved their cybersecurity asset management challenges.***

"WE NOW KNOW ANY TIME THERE'S AN ANOMALY THAT ***NEEDS ATTENTION."***

A uniform, homogenous asset environment would be ideal – but most organizations find reality to be far from it.

This was the case at mobile attribution and analytics company AppsFlyer, where fast growth and the sheer nature of business meant an environment that was anything but uniform. Headquartered in San Francisco, California with over 1,000 employees, these inconsistencies made it difficult for the security team to verify that the right solutions were located where AppsFlyer needed them to be, and that users had permissions in-line with the organization's policies.

>>> WITH AXONIUS, APPSFLYER WAS ABLE TO QUICKLY AND EASILY IDENTIFY WHICH DEVICES DIDN'T ADHERE TO SECURITY POLICIES. THE TEAM ALSO GAINED AN IN-DEPTH LOOK AT VULNERABILITY DATA FOR ALL DEVICES.

The AppsFlyer team faced a challenge when it came to validating that security solutions were appropriately deployed and users had correct permissions across the organization.

APPSFLYER HIRES ITS FIRST CISO TO LAUNCH A THOROUGH SECURITY PROGRAM

January **2018**

APPSFLYER IMPLEMENTS THE BEST SECURITY TOOLS ACROSS DEVICES, BUT LACKS VISIBILITY INTO OVERALL ASSET SECURITY

APPSFLYER CONNECTS THEIR SOLUTIONS TO THE AXONIUS CYBERSECURITY ASSET MANAGEMENT PLATFORM

April **2018**

APPSFLYER INSTANTLY SEES ALL DEVICES – BOTH MANAGED AND UNMANAGED – TO TAKE ACTION AND CORRECT DISCREPANCIES

AppsFlyer chose the Axonius Cybersecurity Asset Management platform to get clear visibility into the deployment of different security solutions and automate ongoing security policy adherence.

"The Axonius solution was dead simple to deploy, and I can't say enough about the team and how quickly they responded to new feature requests or improvements."

- Guy Flechter, former CISO, AppsFlyer

Read the Case Study

cimpress

***"WE NOW HAVE INSIGHT** WHERE WE DIDN'T HAVE IT IN THE PAST."*

Security teams in organizations with highly distributed environments are often challenged with making sense of fragmented data.

With 11 separate businesses, 12,000 employees, and a highly decentralized network all operating under the same umbrella, it's a struggle the security team at Cimpress plc knew all too well. The team was plagued by data inaccuracies and collection issues, leaving them unable to identify gaps in coverage and quickly remediate incidents and vulnerabilities.

>>> **WITH AXONIUS, CIMPRESS WAS ABLE TO EASILY AUTOMATE ASSET DISCOVERY, IDENTIFY GAPS, AND ENFORCE SECURITY COVERAGE.**

AS A GLOBAL ORGANIZATION WITH HEADQUARTERS IN IRELAND AND OFFICES WORLDWIDE, THE CIMPRESS SECURITY TEAM STRUGGLED TO GAIN ASSET VISIBILITY ACROSS THE ORGANIZATION. IT ALSO WAS CHALLENGED BY IDENTIFYING AND REMEDIATING COVERAGE GAPS IN SECURITY POLICIES.

By connecting to the adapters within the Axonius Cybersecurity Asset Management platform, Cimpress automated asset discovery to create one clean inventory – allowing them to double EDR coverage and dramatically reduce incident response time.

"Axonius has been able to give us insight where we didn't have it in the past... If you don't know the assets that you have in your environment and how up to date they are, then you're going to want to take a look at Axonius."

- Daniel Fabbo, Manager of Security Engineering, Cimpress

cimpress

THE CIMPRESS SECURITY TEAM IS TASKED WITH CONNECTING 11 DISPARATE INFRASTRUCTURES

July **2018**

PLAGUED BY DATA ACCURACY AND COLLECTION ISSUES, CIMPRESS STRUGGLES TO IDENTIFY GAPS IN ANTIVIRUS AND EDR COVERAGE, LOCATE INCIDENTS AND VULNERABILITIES, AND RESPOND QUICKLY.

CIMPRESS USES THE AXONIUS CYBERSECURITY ASSET MANAGEMENT PLATFORM TO CONNECT DISPARATE SYSTEMS AND AUTOMATE ASSET DISCOVERY.

November **2019**

CIMPRESS INCREASES EDR DEPLOYMENT COVERAGE TO 80% AND REDUCES PERSON HOURS NEEDED TO INVESTIGATE INCIDENTS WITH AXONIUS.

THE CIMPRESS IT TEAM CREATED QUICK QUERIES TO OVERCOME THEIR VISIBILITY CHALLENGES. INSTEAD OF SPENDING HOURS WRITING AND LAUNCHING SCRIPTS TO GATHER INFORMATION, AXONIUS IMMEDIATELY PROVIDED VISIBILITY.

Read the Case Study

mindbody

"WE'VE ACHIEVED AN OVERALL MATURITY OF ***ABOVE FOUR (OUT OF FIVE)."***

It's an ever-present problem in cybersecurity: Asset management is foundational, and yet so often existing approaches leave us with limited visibility and gaps in our security coverage.

Global SaaS provider for the health, beauty, and wellness industry, Mindbody was familiar with this cybersecurity song and dance – and they'd had enough. In an effort to obtain centralized visibility and data, reduce blind spots, and drive response capabilities, the organization – which has over 1,500 employees – chose Axonius.

>>> **WITHIN JUST DAYS OF IMPLEMENTATION, MINDBODY REALIZED IT HAD DISCOVERED AN IDEAL OUT-OF-THE-BOX CYBERSECURITY SOLUTION THAT PROVIDED THE CLARITY THEY SO DESPERATELY SOUGHT.**

mindbody

The security team at Mindbody was struggling to establish a comprehensive view of what was in and running on their network and to eliminate blind spots for incident response.

With Axonius, they were able to see everything in its environment – despite disparate systems and teams. This enhanced visibility meant expanded incident response capabilities and an overall cybersecurity maturity rating of above four (on a zero to five scale).

Mindbody's cybersecurity maturity rating after deploying Axonius

Amount of time it took for Mindbody to get Axonius up and running

> **"Axonius... solved our cybersecurity inventory problem for us. We moved pretty fast with it because of the ease of use... Within a couple of weeks, we had it at 75 percent efficacy."**
>
> *- Jason Loomis, CISO, Mindbody*

Read the Case Study

FORTUNE 500 ENERGY MANAGEMENT COMPANY

"ASSET MANAGEMENT IS THE FOUNDATION FOR ALL OUR SECURITY CONTROLS."

Thanks to the explosion of mobile and IoT, already complex environments are growing more complicated by the hour.

The proliferation of these ephemeral devices adds a new, unprecedented degree of complexity that security teams are left scrambling to solve: How do you account for and secure these devices when you often can't even identify them in real-time?

>>> **ONE ENERGY MANAGEMENT COMPANY WAS FACED WITH A DEVICE FRAGMENTATION AND DISCOVERY PROBLEM – MADE EVEN MORE COMPLICATED BY THE SHEER SIZE AND BREADTH OF THE ORGANIZATION.**

By choosing Axonius, this manufacturing organization was able to automate asset discovery – even when it came to ephemeral devices – and accelerate incident investigation and response.

FORTUNE 500 ENERGY MANAGEMENET COMPANY

A global Fortune 500 energy management company with operations in over 100 countries and more than 500,000 employees worldwide was having difficulty identifying and tracking assets – especially those that are ephemeral in nature – in its environment. It was also challenging for the organization to correlate alerts and IOCs with asset information, meaning lagging response times when it came to incidents.

With Axonius, the company's security team was able to automate asset discovery and speed up the incident investigation process from three to five days to three to four hours – ***nearly a 90 percent decrease in time.***

"Axonius has become a pretty critical piece of our whole ecosystem."

- Director of Enterprise IT Global Security, Global Energy Manufacturing Company

FORTUNE 500 ENERGY MANAGEMENT COMPANY

10 DAYS

Time it took to onboard with Axonius, connect all data sources, and correlate a comprehensive asset inventory

90%

Decrease in time to conduct incident investigations using Axonius

3 HOURS

Time it now takes to complete investigations using Axonius

The team at this global energy management company used Axonius to break down and eliminate data silos.

THIS PROVIDED VARIOUS SECURITY TOOLS AND TEAMS WITH UNIFIED ACCESS TO A WEALTH OF DATA THAT WASN'T PREVIOUSLY AVAILABLE.

Read the Case Study

Landmark

*"WE'VE PUT COMPLIANCE ON **AUTOPILOT."***

Traditional approaches to compiling asset inventory data for security audits are exceptionally manual, often relegated to Excel workbooks and V-LOOKUPs. It's a process that, while essential, is labor intensive and prone to error.

And at Landmark Health, it's a process that was eating up hours of the security team's time and leaving them with asset inventories that were out-of-date at best.

>>> **WITH AXONIUS, THE LANDMARK TEAM SHIFTED FROM ONCE-QUARTERLY AUDITS TO DAILY AUDITS, AFFORDING THE SECURITY TEAMS' CONFIDENCE AND PUTTING THEIR COMPLIANCE ON AUTOPILOT.**

Landmark

Landmark Health was manually validating that solutions were appropriately deployed for compliance and software license management.

By using the Axonius Cybersecurity Asset Management platform to automate policy validation, Landmark Health is now able to ensure each device meets compliance requirements. The company has also increased its security posture and eliminated time-consuming, manual audits.

> **"There has never been a tool that does what Axonius does, allowing us to tie everything together using simple queries and then putting compliance on autopilot."**
>
> *- Jeffrey Gardner, former Director of Information Security, Landmark Health*

BEFORE AXONIUS	***WITH*** AXONIUS
Failed red team exercises	Cybersecurity ***confidence***
Audits ***once per quarter***	Automated ***daily audits***
Manual policy compliance	Compliance on ***autopilot***

Read the Case Study

AXONIUS

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.

330 MADISON AVE., 39TH FLOOR
NEW YORK, NY 10017
INFO@AXONIUS.COM

See what other customers have to say about the Axonius Cybersecurity Asset Management platform.

Read real reviews on Gartner Peer Insights.

READ REVIEWS

Gartner peerinsights™