AXONIUS

EBOOK

The 6 Most Common Asset Management Challenges for Cybersecurity

WHY THEY MATTER AND HOW TO SOLVE THEM

> I’ve lived the pain of never getting a straight answer about assets. We never know how many servers there are, virtual machines, endpoint devices. And before we start worrying about ninjas chasing us with APTs, we should first try to solve something that is as basic, yet foundational as asset management.

Patrick Heim

Operating Partner and CISO, Clearsky

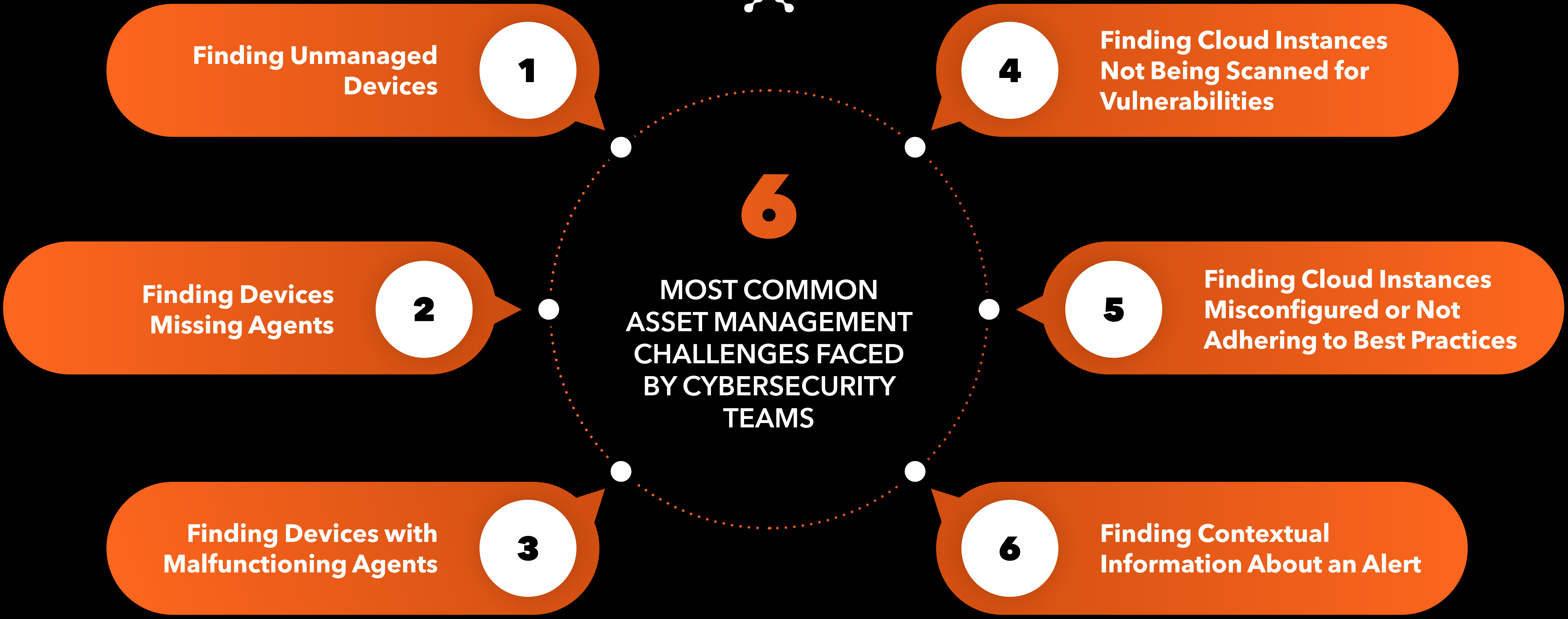
Despite the incredible technologies available in cybersecurity today – from deception to automation, AI to machine learning – security teams **still struggle to get accurate answers** to asset-related questions.

And while the tools we use can give us individual pieces of the asset puzzle, information lives in many different silos.

This makes it hard to ask simple questions that span the many data sources.

Read on to learn:

- **The unique challenges caused by assets**
- **Why these hurdles matter from a cybersecurity perspective**
- **The data sources required for asset management**
- **How to solve each challenge with cybersecurity asset management**



6 MOST COMMON ASSET MANAGEMENT CHALLENGES FACED BY CYBERSECURITY TEAMS

1 Finding Unmanaged Devices

2 Finding Devices Missing Agents

3 Finding Devices with Malfunctioning Agents

4 Finding Cloud Instances Not Being Scanned for Vulnerabilities

5 Finding Cloud Instances Misconfigured or Not Adhering to Best Practices

6 Finding Contextual Information About an Alert

Click on any challenge to jump to a detailed page

CHALLENGE 1

Finding Unmanaged Devices

What Do We Mean By "Unmanaged Devices"?

Unmanaged devices are endpoints (laptops, desktops, servers, IoT devices, etc.) that aren't known to management systems and don't have an agent installed. These are devices that aren't being controlled or managed by an organization's security and configuration management tools.

The Challenges

Organizations today have a comprehensive arsenal of security tools to protect corporate-assigned devices. But those tools can only protect the assets they know about. Finding the "unknown unknowns" poses a huge challenge.

Asking Active Directory (AD) to show any unmanaged device doesn't work. Manually comparing AD data and network management and endpoint security software is time-consuming and error-prone.

Continuously discovering unmanaged devices automatically requires correlating and deduplicating data from multiple sources to uncover risks to quickly address them. Finding unmanaged devices involves triangulating data from multiple sources to understand the difference between:

- Devices known to the network
- Devices without a security agent installed
- Devices without a management agent or configuration solution installed
- Devices known by IAM solutions

Simply put, finding unmanaged devices is tricky.

The Implications for Cybersecurity

If a device is unmanaged, it's impossible to know if it's secure. Data from the network infrastructure or network scanners can yield scant details – sometimes just an IP address.

Since very little is known, how can you distinguish between a smart TV in the conference room (which isn't going to be part of a patch schedule) and a Raspberry Pi with open ports? The first step in securing, managing, segmenting, and controlling any device is to first understand what that device is and its context.

Data sources needed to find unmanaged devices:

IAM Solutions
Services like Active Directory or Azure AD that authenticate and authorize users and devices

Device Management Solutions
Services like SCCM and Jamf Pro

Network/Infrastructure Data
By connecting to the networking infrastructure, administrators gain visibility into all devices within their environment

Endpoint Protection Solutions
Endpoint security agents installed and protecting devices

For more detailed information, read Finding Unmanaged Devices.

How to Find Unmanaged Devices

Finding unmanaged devices is one of the most basic functions of an effective asset management program. It results in a comprehensive list of devices that are either:

- Unmanaged and *can* be managed
- Unmanaged and *can't* be managed

Given data from the sources listed on this page, finding unmanaged devices is an exercise of comparing data from:

Network/Infrastructure Data
Look at all of the IP addresses from network infrastructure to see all devices that have accessed network resources

IAM Solutions
See the subset of devices that aren't being centrally managed

Device Management Solutions
Review all devices that aren't being updated and monitored for configuration changes

Endpoint Security Solutions
Understand which devices lack the expected security agent

First, start with a full list of all devices that have accessed network resources.

Then, filter out those devices with the appropriate security and management tools installed. You'll end up with a candidate set of unmanaged devices.

But that's only the beginning. Next, you'll need to understand the context of each device.

Things like IoT devices and IP phones may be "unmanaged", but you can't drop an .exe on them as though they were laptops. So you'll then need to identify the device type and filter out those that are unmanaged and can never be managed.

Here's how to find unmanaged devices:

1. Gather all device data from the network, IAM solutions, device management consoles, and endpoint security agent solutions.
2. Map out the overlap and gaps between those devices that have accessed network resources and those that have an agent installed.
3. Of those devices without an agent installed, identify the device context and filter out those that can't have an agent installed (IP phones, webcams, IoT devices, etc.).
4. Aggregate your list of unmanaged devices that should be managed, then prioritize agent and management system deployment and coverage.
5. Develop a process that continuously monitors for new, unmanaged devices, then repeat the steps above.

Once armed with this context, you can move on to remediation action.

> "Finding unmanaged devices is one of the **most basic functions** of an effective asset management program."

CHALLENGE 2

Finding Devices Missing Agents

What Do We Mean By "Devices Missing Agents"?

We're referring to devices (physical, virtual, or cloud) expected to have an endpoint agent installed. Whether a security agent (like an endpoint protection tool) or a configuration management agent, these are lightweight applications installed at the operating system level on a corporate endpoint.

Agents generally run continuously and silently in the background. They gather data about the state of the device and use that data to evaluate whether any changes impact its expected security posture, performance, or behavior.

When organizations mandate that specified devices have agents installed, a device missing an agent is one that doesn't have the expected agent installed.

This is an important distinction – there's a difference between a device missing an agent and a device with the agent present but not functioning (we'll cover this later).

The Challenges

Many organizations standardize on several agent-based tools in these ways:

Functionality
Examples include security tools to prevent malware and configuration management tools to ensure machines are up to date.

Device Type
Some endpoint agents are device type specific, with one tool for computers, others for mobile devices, etc.

Operating System
A solution that covers Windows devices may not work on Mac and Linux endpoints.

If the goal is to simply understand which devices have a specific endpoint agent installed, you can access the admin console of the agent to produce a list of covered devices.

But that doesn't solve the problem here: which devices should have the agent, but don't?

Part of the challenge is due to device discovery. How does an EPP/EDR solution identify a new device that exists and should be protected? The other issue is based on the context of the security policy.

For example, if my security policy requires one endpoint agent for PCs and another for Macs, what mechanism is in place to find the device? Understand its context? Ensure the right agent is installed to meet the policy?

Data sources needed to find devices missing agents:

IAM Solutions
Services like Active Directory or Azure AD that authenticate and authorize users and devices

Device Management Solutions
Services like SCCM and Jamf Pro

Endpoint Protection Solutions
Endpoint security agents installed and protecting devices

The Implications for Cybersecurity

As a cybersecurity leader, think of all of the time and effort you dedicate to researching, evaluating, negotiating, and then deploying an agent-based security tool.

Then think about getting hit with a security incident or breach caused by a machine that didn't have the agent installed.

Painful to consider, right?

You've already determined the right toolset to secure and manage devices.

You've purchased the solutions. But without knowing that all relevant devices are covered, it's impossible to be confident that you're really protected.

How to Find Devices Missing Agents

Given data from the sources listed on the previous page, finding devices missing agents requires comparing data from:

IAM Solutions
See devices that are centrally managed

Device Management Solutions
Look at all devices with the specified agent installed

Endpoint Security Solutions
Understand which devices have the expected security agent installed

For more detailed information, read Finding Endpoints Missing Agents

Using this data, you'll need to understand:

1. **Which devices/types should have a certain agent installed**
   For example, if every Windows device needs to have CrowdStrike installed and every Mac needs JAMF
2. **Which devices have the correct agent installed**
   To see the full set of devices properly covered
3. **The delta between points one and two in this list**

To find devices missing endpoint agents, let's take one example: Windows machines that should have CrowdStrike installed. To get to that data, we:

1. **Find every Windows device**
   Starting from the full set of devices in our inventory, we need to focus on those running Windows. To do that, we'll need to gather data from a source that can give us OS information.
2. **Find every Windows device running CrowdStrike**
   We can then look at the CrowdStrike admin console to see every Windows device that has the CrowdStrike agent installed.
3. **Parse the delta**
   Subtract all of the Windows devices running CrowdStrike from the full list of Windows devices. We're now left with the full set of devices that should have the agent installed but lack the agent coverage.

We would then need to repeat these steps for any agent on any device type:

- Macs missing JAMF
- Linux missing BigFix or Chef
- Windows missing Tanium or SCCM

These are just a few examples. You'll need to fill in your own solutions and run through the above steps for each. You'll then need to continuously run through this process for every new asset added to your environment.

CHALLENGE 3

Finding Devices with Malfunctioning Agents

What Do We Mean By "Devices with Malfunctioning Agents"?

We're referring to those devices that have the agent installed, but it's either not active or not sending back data as expected.

The Challenges

Logging into the admin console of any agent-based solution will give you a list of devices on which the agent is installed. You'll also be able to find a "last seen" date, letting you know when the agent has sent data back to the mothership.

You won't, however, be able to see if the agent has been turned off, if it was uninstalled by the user, or if it's simply not functioning correctly.

The Implications for Cybersecurity

Apart from knowing which devices aren't being protected by knowing an agent is missing, we also need to know whether the agent is working. A binary "here/not here" doesn't tell us whether that agent is functioning.

If we stop once we know which devices have an agent installed, then we won't be able to account for cases where the agent is there, but just isn't working properly.

For more, read Finding Endpoint Agents Not Functioning Correctly

How to Find Devices with Malfunctioning Agents

To find devices with malfunctioning agents, we need to:

1. **Find all devices with the agent installed**
   Look at the agent console to get the information on those devices covered.
2. **Get the subset of devices with a "stale" last seen date**
   For example, show me every device that hasn't been seen by the agent console in more than 30 days.
3. **Get the devices seen by other solutions within 30 days**
   If a device that has the agent installed hasn't transmitted data to the agent console in 30 days, but has been seen by AD or another agent console in the last week, we can assume the device's agent is either off or malfunctioning.

Data sources needed to find devices with malfunctioning agents:

Endpoint Agents
By connecting to the agent's admin console, you can see all devices that have the agent installed, along with a "last seen" date/time. These could be:

- AV Agents
- EPP/EDR Agents
- Systems Management and Configuration Agents

IAM Solutions
Services like Active Directory or Azure AD that authenticate and authorize users and devices.

CHALLENGE 4

Finding Cloud Instances Not Being Scanned for Vulnerabilities

What Do We Mean By "Cloud Instances Not Being Scanned for Vulnerabilities"?

We're referring to public cloud infrastructure services – like those from AWS, Google Cloud, and Microsoft Azure – that organizations want to scan for known vulnerabilities.

The Challenge

Today's assessment tools do an exceptional job of recognizing known vulnerabilities. But thanks to their elastic and ephemeral nature – and the increasing adoption of DevOps methodologies – cloud workloads are spun up and down without security tools ever being aware of their existence.

This means tools like VA scanners are often unaware of any new instances to scan, making these instances prone to known vulnerabilities. VA scanners only know to scan IPs they have been given to scan, and the dynamic nature of the cloud makes it impossible for these tools to anticipate new IPs. Simply specifying an IP range won't work.

The Implications for Cybersecurity

Put simply, cloud instances not being scanned are at risk of being exploited. And publicly accessible cloud instances not being scanned add another layer of risk. A simple Google search shows just how often breaches occur due to publicly accessible cloud instances.

How to Find Cloud Instances Not Scanned for Vulnerabilities

To find cloud instances not being scanned by a VA scanner, we must:

1. **Find all cloud instances**
   We'll look to the public cloud infrastructure provider(s) to get the full list of all active instances.
2. **Find every cloud IP being scanned**
   Looking at our VA scanner coverage, we'll see all IPs that are part of the scan schedule.

Once we complete steps one and two, we'll use that information to find those active cloud instances that are unknown to our VA scanner. We'll need to complete these same steps for every cloud provider and every scan-based tool. Then, we'll need to continuously run the same process for every new cloud instance.

Data sources needed to find cloud instances not being scanned:

Vulnerability Scanner Console
Connecting to the admin console of the vulnerability scanner allows you to see all cloud instances that are known and being scanned.

Cloud Infrastructure
Connecting to the cloud infrastructure admin console allows you to see all instances in the environment.

The delta between known cloud instances and those known to the VA scanner yields those not being scanned.

For more, read Discovering Cloud Instances Not Being Scanned For Vulnerabilities

CHALLENGE 5

Finding Cloud Instances Misconfigured or Not Adhering to Best Practices

What Do We Mean By "Finding Cloud Instances Misconfigured or Not Adhering to Best Practices"?

This implies a standard set of proper configuration options that should be adhered to. In this case, we'll refer to the CIS Foundations Benchmarks for public cloud providers.

The CIS Foundations Benchmarks provide a list of best practices around things like identity and access management, logging, monitoring, and networking to ensure that each cloud instance is properly secured. Misconfigured instances, therefore, are those that fall short of these guidelines.

The Challenge

Cloud providers offer instant scalability and forecastable cost structures, letting teams spin workloads up and down any time. But the nature of the cloud means that workloads can be – and often are – publicly available. In some cases, like with a web server, making resources publicly available is the point. But if a misconfiguration results in an S3 bucket leaking customer records... well then, that's a problem.

The many configuration customization options of public cloud workloads, coupled with the dynamic ability to create massively scalable instances, makes it increasingly difficult for security teams to discover when a new cloud instance arises at all – much less a new instance that's also misconfigured and vulnerable.

The Implications for Cybersecurity

Since the cloud is public, and cybercriminals can automatically scan for publicly accessible instances, it's no wonder that when researchers left a poorly configured database open to the internet, it only took eight hours for the attacks to start.

How to Find Cloud Instances Not Adhering to Best Practices

1. **Gather data from cloud infrastructure provider APIs**
   Get all cloud instances currently available, along with settings and configuration options.

2. **Compare configuration details to the benchmark**
   Map each configuration setting to the scored rules within the CIS Foundations Benchmark for each cloud provider. See all accounts and instances that both adhere to or deviate from the rules stated in the benchmark.

Though a fairly simple concept, the difficulty is knowing any time a new instance exists, running through the benchmarks to compare, and monitoring for all relevant configuration changes over time for all cloud providers.

Data sources to find misconfigured cloud instances:

Public Cloud Infrastructure Admin Data
Access to the AWS, Azure, GCP, and other public cloud providers to show all current cloud instances and their configuration details.

Industry Benchmarks like CIS Foundations Benchmarks
To see the commonly-accepted industry best practices for configuration details.

For more detailed information, read Cloud Asset Compliance

CHALLENGE 6

Finding Contextual Information About an Alert

What Do We Mean by "Contextual Information About an Alert"?

An alert from a detection solution may include an IP address, a time, an indicator, and a few other data points. When an analyst sees an alert, they immediately need to discover more context. They'll ask questions like:

- What machine is at that IP address?
- Where is it?
- What's on it?
- What does that machine have access to?
- What user is logged in?
- What is the machine's purpose?
- What known vulnerabilities exist?

The Challenge

The analyst who gets the alert likely won't have immediate access to the asset data that would provide valuable context.

It can be both manual and time-consuming to identify the data owners, understand the systems and controls related to the asset, and get a full view of the asset, including its state and risk.

The Implications for Cybersecurity

The moment an alert comes in, the clock starts ticking. Any alert is a potential indicator of an incident or breach. The sooner it can be investigated and remediated, the lower the risk and subsequent impact.

For more detailed information, read Accelerate Incident Response Investigations.

How to Find Contextual Information About an Alert

1. **Identify the endpoint from the alert**
   The alert may just have an IP address, or it may have IP and hostname.
2. **Gather data from security and management solutions**
   These could include agent-based tools, VA scanners, NAC solutions, IAM tools, networking gear, firewalls, and more.
3. **Correlate the information**
   Understanding which tools cover which assets will reveal patch status, known vulnerabilities, and the overall state of the asset at the time of the alert.

Armed with this context, IR teams can quickly learn whether the alert is indicative of a larger problem, what needs to be remediated, and whether other endpoints are at risk.

Data sources needed for alert context:

Endpoint Agents
These can provide rich information on devices, including running software, OS type and version, external IP, network interfaces, and more.

Configuration Patch Management
Configuration and patch management agents like Tanium provide rich device information.

Ticketing and Help desk platforms
Platforms like ServiceNow and ZenDesk often provide information like device location, associated department, first and last discovery date, and more.

Networking
Understand where the device is located on the network and where it's been.

Vulnerability Assessment Tools
Discover if the device had known vulnerabilities that may have been exploited

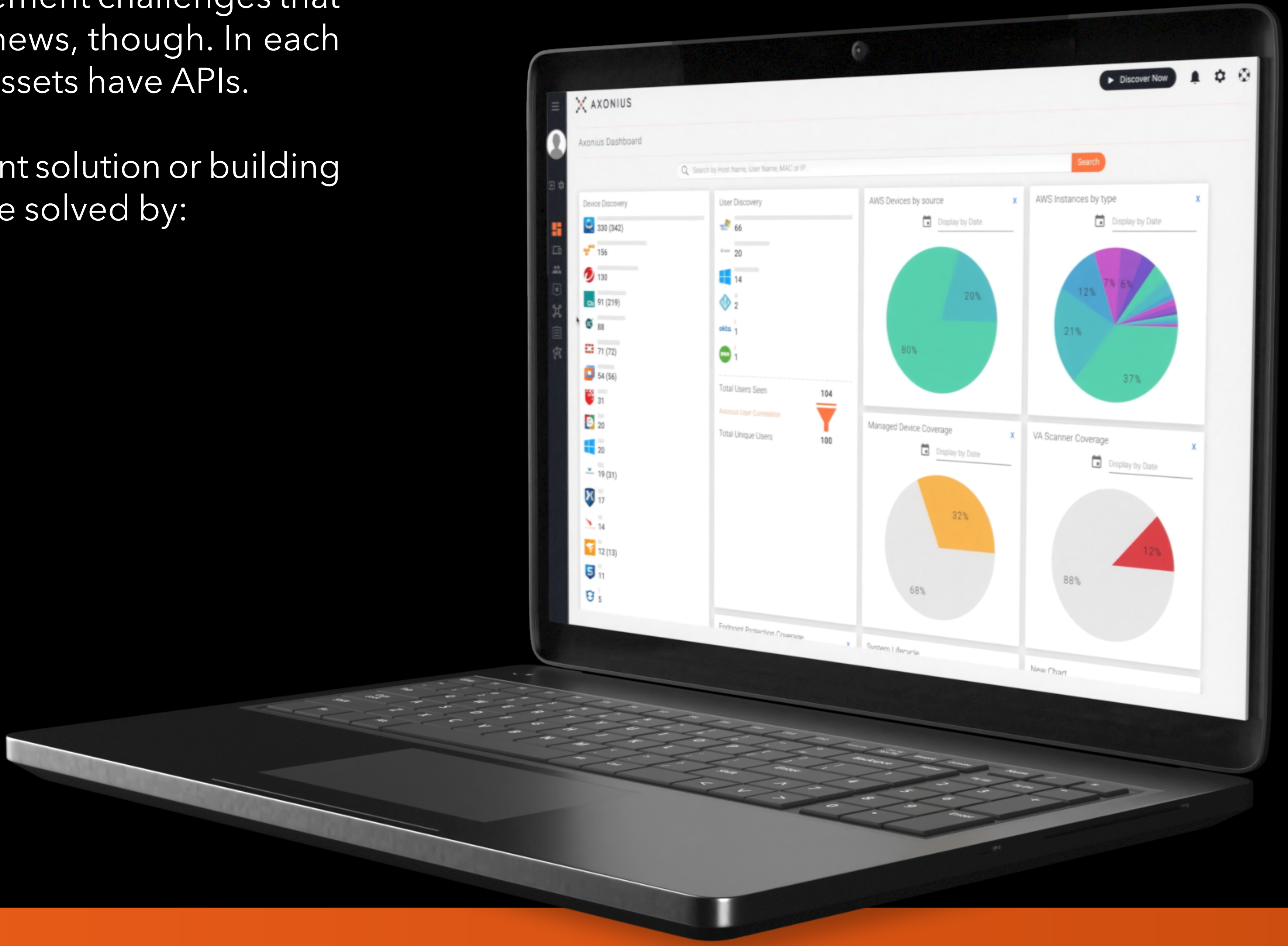
IAM Solutions
Learn user privileges, whether the device is enrolled in MFA, password strength and expiration, and more with services like Active Directory, Okta, or Azure AD.

Solving Asset Management Challenges for Cybersecurity.

These six common questions are just a few of the asset management challenges that security teams are most frequently up against. There's good news, though. In each case, all the data is there – and the solutions that know about assets have APIs.

Whether you're implementing a cybersecurity asset management solution or building something in-house, each asset management challenge can be solved by:

1. Gathering data from any source that knows about assets
2. Correlating the data to ensure that the solutions are referring to the same unique device
3. Understanding the relationship between the asset and its solution coverage
4. Querying across all data to get answers to questions
5. Running continuous queries to know any time a new asset appears and when an asset changes



See your assets in context, validate security policy compliance, and automate remediation with Axonius' cybersecurity asset management platform.

SEE IT FOR YOURSELF

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 250 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

AXONIUS.COM ©