AXONIUS

The 1st Step to Zero Trust: Asset Management for Cybersecurity

"If I have 20 calls, 17 are about Zero Trust. CISOs, CIOs and CEOs are all interested, and companies of various sizes are interested. And in three years, I think Zero Trust will be cited as one of the big-time frameworks in cyber security. Period."

Chase Cunningham
Principal Analyst, Forrester

OVERVIEW

Eight years after former Forrester analyst John Kindervag introduced the Zero Trust model, the concept has hit the mainstream. As current Forrester analyst Chase Cunningham says, 85% of his calls involve zero trust. With the amount of interest in the concept, many organizations are rushing to understand how to implement the zero-trust model. In this guide, we'll look at the first step to implementing zero trust: asset management.

Table of Contents

The Evolution of Zero Trust

Wendy Nather, Director, Advisory CISOs at Duo security in a video interview during RSA 2018 concisely explained the following evolution of the Zero Trust model:

- 2003 - "The Jericho Forum - a bunch of financial services CISOs - got together in the UK and started talking about how we really shouldn't trust anything just because it's inside the perimeter. They proposed a collaborative architecture, and I remember at the time reading about it and saying, 'that sounds great, but how in the world would you do that?'."

- 2009 - "John Kindervag (when he was a principal analyst at Forrester) coined the term 'Zero Trust' and how you might implement that according to his model within the enterprise."

- 2014 - "Google had figured out how to implement the model inside of their organization and started issuing white papers and doing talks about how the implemented it, and they called their model BeyondCorp. Especially when Google sat up and said 'this is how we did it,' people started to see that it was within reach in their organizations as well, and it gained steam from there."

What is Zero Trust?

Zero Trust is a security concept centered on the belief that organizations **should not automatically trust** anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

While traditional information security approaches used the castle-and-moat analogy that focuses on defending a perimeter and assumes anything on the inside is safe, the Zero Trust model makes no assumption based on position relative to perimeter. Just because a user or asset has made it onto the corporate network does not automatically infer a level of confidence.

Examples about to show that the castle-and-moat approach doesn't work. From the smart fish tank that left a casino vulnerable to cyber criminals to the oft-cited Target breach caused by compromised credentials from an HVAC company, examples abound showing how much damage can be caused by trusting users and systems that have crossed the moat and were considered trustworthy.

"In working with some of the largest companies on earth, I've seen countless cases where a trusted user or device could completely take down a corporate environment," said Dean Sysman, CEO and Co-Founder at Axonius. "For example, I've seen Fortune 500 companies that have service accounts with full admin access to every machine in the organization. Coming from an offensive background, I can tell you with confidence that if a malicious actor gained those credentials, it's game over. You would literally need to start over and rebuild the network from scratch."

The threat of bad actors and high-profile breaches alone are compelling reasons to consider the zero-trust approach. But FUD aside, the most pragmatic driver is the change in the way we work.

In the not-so-distant past, work was a place where people sat in a building with Windows desktops connected to a physical network via ethernet cable. These were people that were trusted employees using corporate sanctioned devices to access information necessary to perform their work. In that world, the castle-and-moat approach made sense: only those workers with physical access to the network were allowed to touch what was within the firewall.

And then things changed.

Trends like cloud, virtualization, BYOD, work-from-home, mobile devices, and IoT have completely transformed the way we work and, in the process, removed the perimeter. Right now, I'm writing this paper on an Amtrak train in route to New York City while logged in to my corporate email running on Google Apps. I'll finish writing using my personal laptop on my home network. Where's the perimeter?

A vastly different computing environment creates a massively distributed attack surface that requires a fundamental rethinking of our security framework.

Technologies Associated with Zero Trust

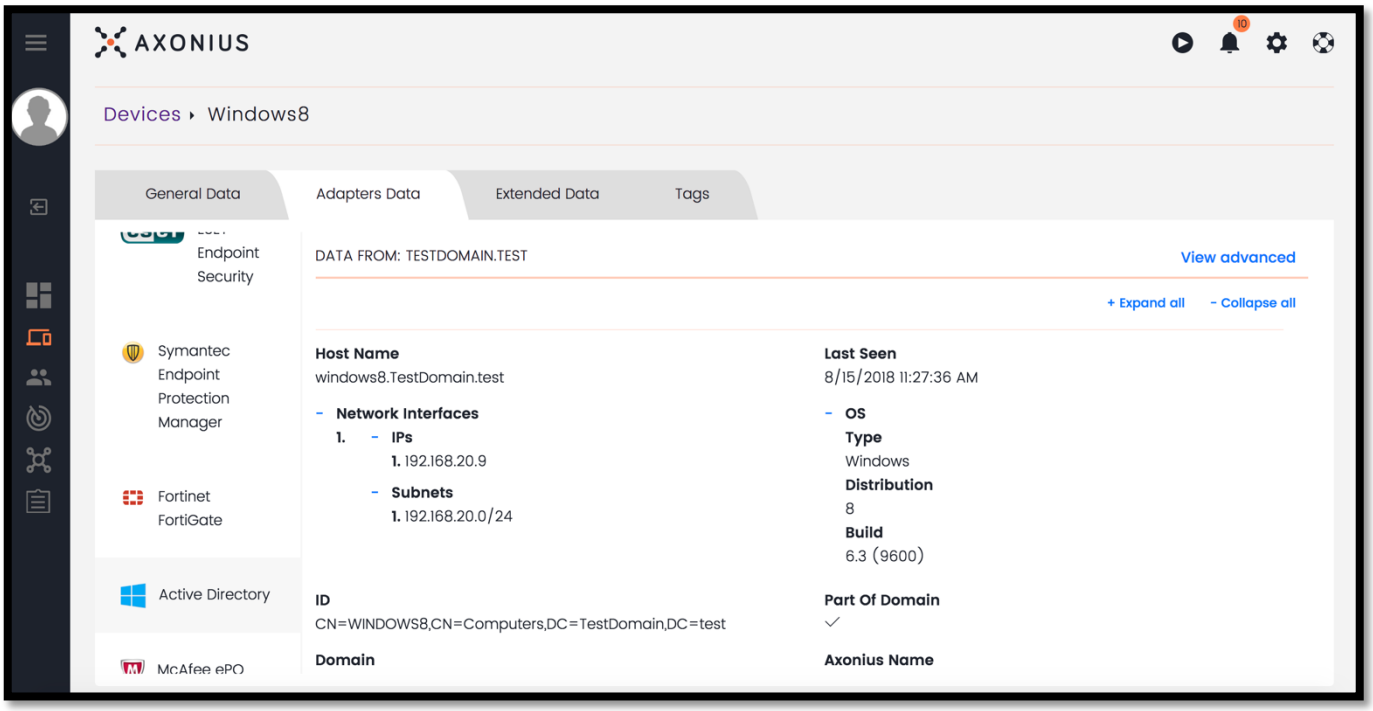
A quick Google search will tell you that nearly every cybersecurity vendor is on the zero-trust bandwagon. With more than 30 million results and rising, the term hasn't leveled off yet. Let's take a look at some of the functional areas associated with zero-trust and the technologies that can help.

1. **What is the device that is trying to access corporate assets?** Is the device in question a laptop? Smart TV? IoT Device? Knowing the type of device is the first in a series of granular questions to ask to determine whether granting access is appropriate. For example, a web-enabled baby monitor probably shouldn't be trying to request data from a file share.
2. **Is the core software up to date?** Assuming a device clears the first hurdle, let's then check to see whether the OS is current. You may not want a laptop running XP to have access to, well, anything really.
3. **Which vulnerabilities exist on the device?** Aside from the core software, what else is installed? What vulnerabilities come with the additional software resident on the device?
4. **Is the device "managed"?** Most organizations mandate that a specified endpoint protection solution is installed on each device, usually with an agent. If that agent isn't installed (or isn't running), you may want to only allow that device on the guest network, and you may want to force an installation of said agent before accessing anything that isn't publicly available.
5. **What user is logged in?** Now that we know about the device, let's figure out the person using it. Is it a network admin? A member of the finance group? Someone that left the company 6 months ago?
6. **Does the user have access?** Finally, let's try to understand whether the user should be able to access what they are requesting.

Let's take a look at some of the technologies that can answer the questions above.

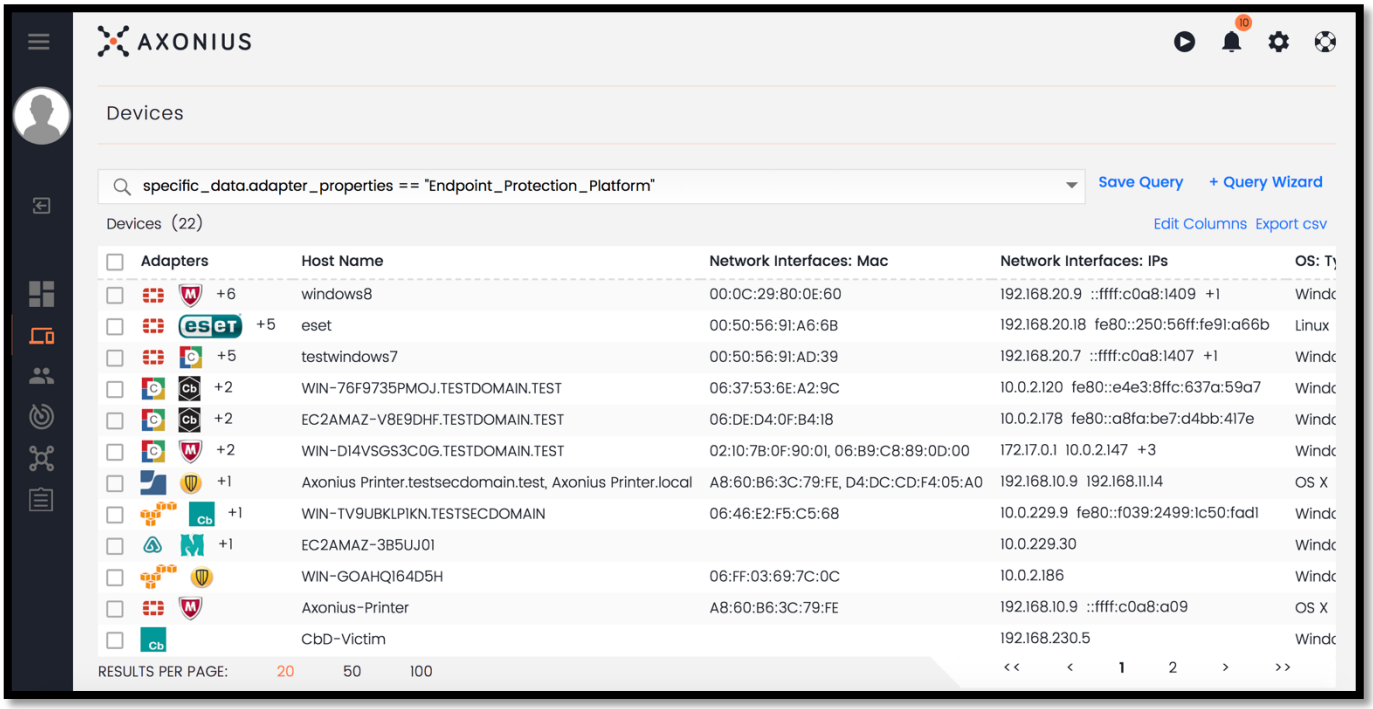
ACTIVE DIRECTORY

Active Directory can help us to understand the device and user roles and how each fits in the organizational policy. At the most basic level, AD can tell us whether a user and device are known and have permission to access any corporate asset. At the most granular, AD can tell us which assets are accessible by looking at group membership and policy adherence.



ENDPOINT PROTECTION

Most organizations mandate that an EDR or EPP solution is installed and running on every endpoint. These solutions can detect, prevent, and remove malicious items like malware before they can move laterally and infect other network assets. Additionally, in a BYOD and remote working environment, cloud-delivered endpoint protection products can be the only way to understand the security status of devices that never connect to a corporate network or VPN.

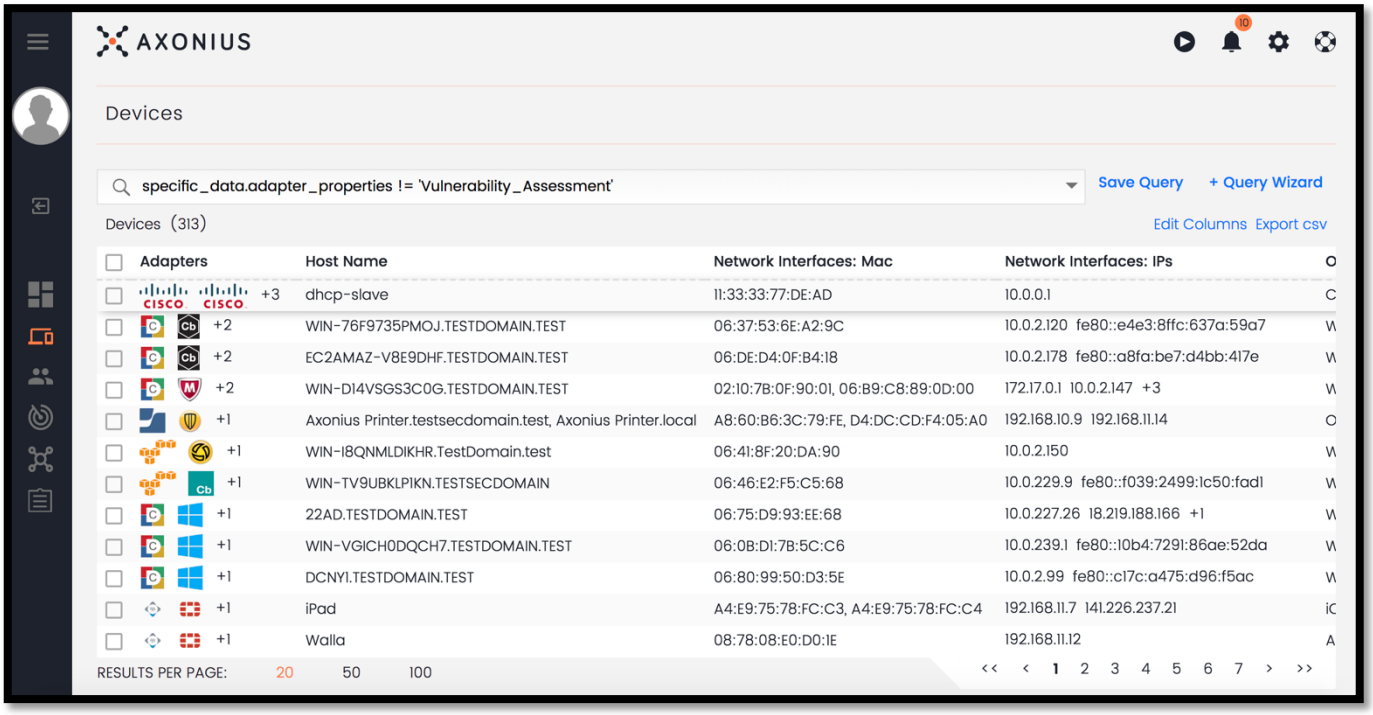


Devices with an Endpoint Protection Platform installed

VULNERABILITY ASSESSMENT

To understand which vulnerabilities are present on any device, organizations us VA tools to compare lists of known vulnerabilities to the version of each application present. Based on the severity of any vulnerabilities found, actions can be taken to either prevent a device from accessing corporate data, or if a patch is available, force an upgrade before granting access.

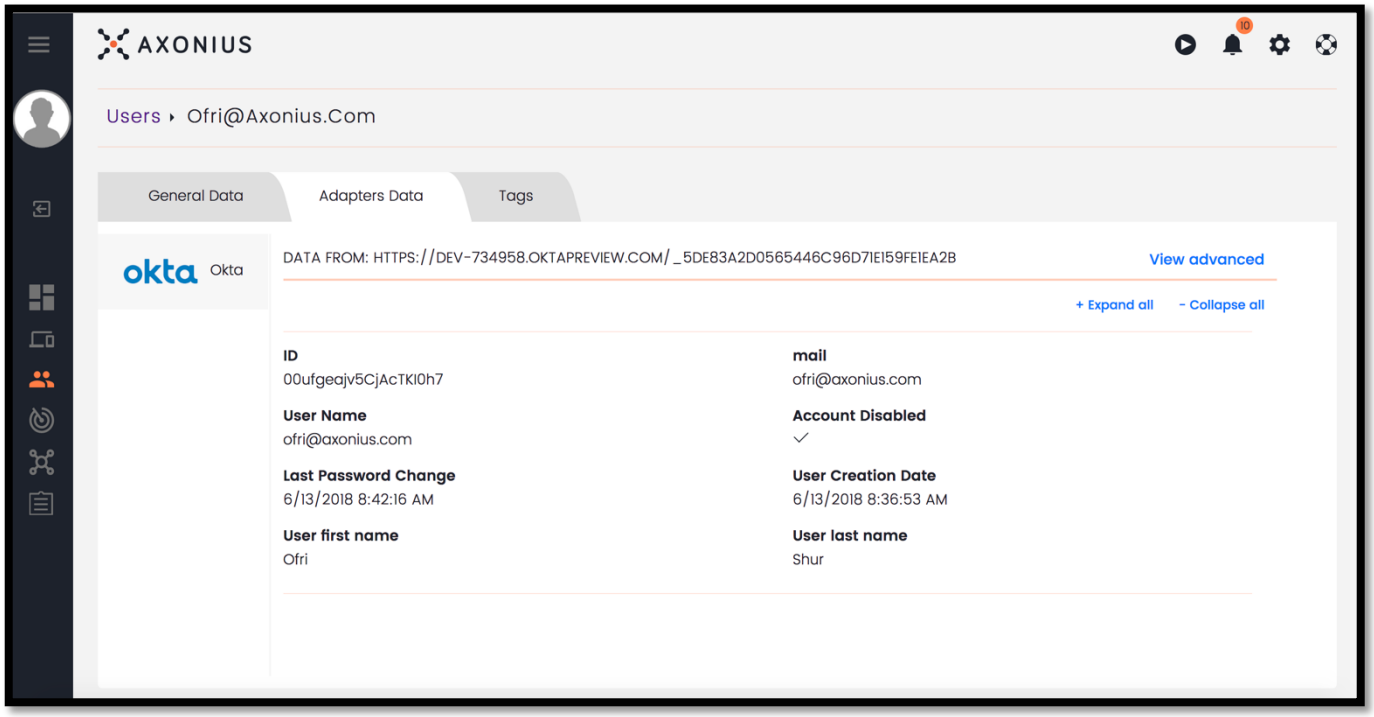
Although some VA tools have discovery capabilities, many will only scan devices that they know about in a given IP range. Because of this, we cannot rely on a result such as “no known vulnerability detected” as a condition to be met, as that requirement could come from a VA tool simply not knowing that a device exists.



Devices that have not been scanned by a Vulnerability Assessment Tool.

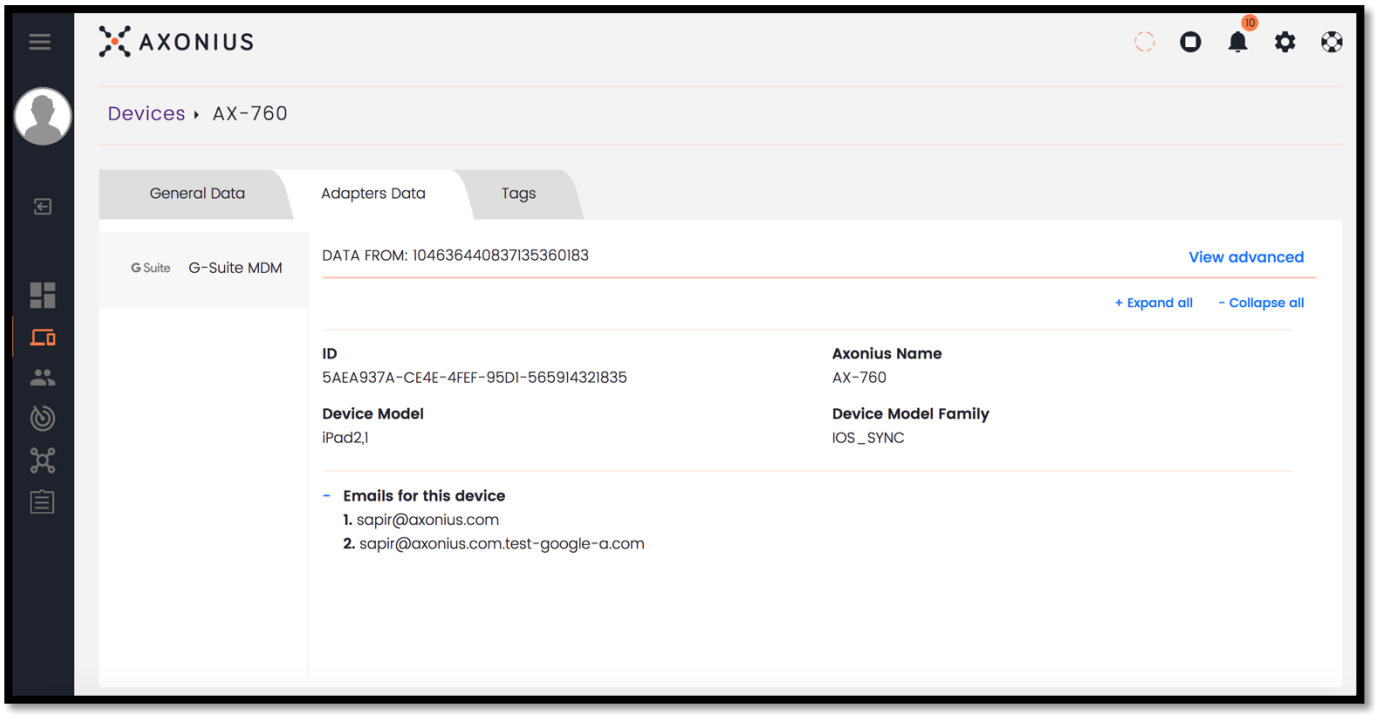
IDENTITY AND ACCESS MANAGEMENT

Aside from Active Directory, many organizations are looking to IAM providers that offer multi-factor authentication and single sign-on for added security and for added convenience. These products can also add application-level permissions for cloud-based services. For example, a company may use AD to authenticate users to access files and corporate email but may use an IAM provider to understand which users should have access to the CRM.



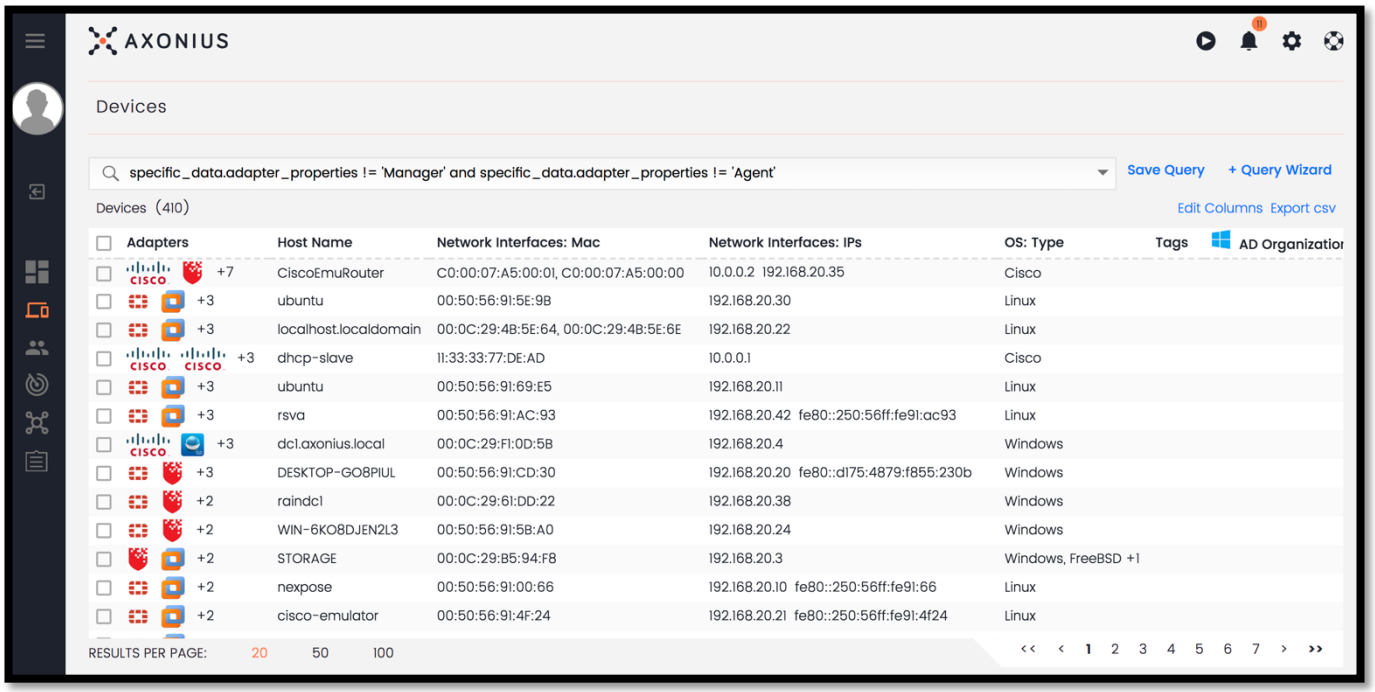
MOBILE DEVICE MANAGEMENT

In an increasingly mobile world, organizations cannot just rely on endpoint protection, as employees use mobile devices constantly, switch devices often, and take their devices with them when they leave. MDM lets companies grant and revoke access at any time without needing physical access to an employee's personal devices.



SWITCHES AND ROUTERS

To understand which devices are unmanaged, we want to look at those devices that are managed (have an agent installed) and compare those to the list of devices known to the switches and routers to find the delta (those IP addresses that are known only to the network without agents installed). This will give us a list of unmanaged devices to create a candidate set to decide which devices should be managed, and those that are unnecessary.



Unmanaged devices known only to the network.

CYBERSECURITY ASSET MANAGEMENT

A relatively new category, cybersecurity asset management products seek to give a comprehensive view into all assets and users to understand the security posture of each. By connecting to all security and IT products in an organization's environment, cybersecurity asset management tools can give a continuous view of the relationship between devices, users, and security product coverage to constantly validate each against the organization's security policy.

A few examples:

- Which devices are unmanaged, but should have an agent?
- What percentage of devices are running our endpoint protection platform?
- Which devices aren't being scanned by our VA tool?
- Which users have improper access rights or passwords that never expire?
- Which of my IoT devices were manufactured in x country?

This new category seeks to use all other security products to correlate data into a single, actionable view.

Implementing the Zero Trust Model

Going from the traditional perimeter-based approach to zero-trust can seem daunting, but it's not an all-or-nothing process. Many organizations approach zero-trust as an aspirational future state, making new security purchasing and implementation decisions with eventual zero-trust in mind.

A few steps organizations can follow to get started on the path to zero-trust:

1. Understand what devices you have.
2. Distinguish between devices that are managed and unmanaged. Then determine which should be managed.
3. Map out security solution coverage and address the gaps.
4. Establish ongoing user access auditing.
5. Implement security policy validation.

UNDERSTAND WHAT DEVICES YOU HAVE

You can only secure what you can see, and until you know which devices are in your environment, it's impossible to know whether those devices are satisfactorily secure. Establishing an ongoing device discovery, classification, and inventory process should be the first step in planning for a zero-trust future.

DISTINGUISH BETWEEN MANAGED AND UNMANAGED DEVICES

A Smart TV in a conference room is different from the CEO's laptop, and they should be treated differently. While the Smart TV doesn't need an endpoint agent or a patching schedule, the laptop does. Creating a process to take action based on asset classification is critical.

ADDRESS THE GAPS IN SECURITY SOLUTION COVERAGE

In our experience, every organization has devices that are missing security solution coverage. Whether that means AWS instances not known to a VA scanner, R&D machines without an EDR solution, or iPhones without MDM, there are always gaps to be addressed. Addressing these gaps in an ongoing basis is a necessity for any organization thinking about zero-trust.

ESTABLISH ONGOING USER ACCESS AUDITING

Are there users in your environment with local admin access to all machines? Users with passwords not required or set to never expire? Service accounts with keys to the kingdom? Even with strict access controls and granular policies, creating an ongoing auditing process is needed to ensure proper access rights.

IMPLEMENT SECURITY POLICY VALIDATION

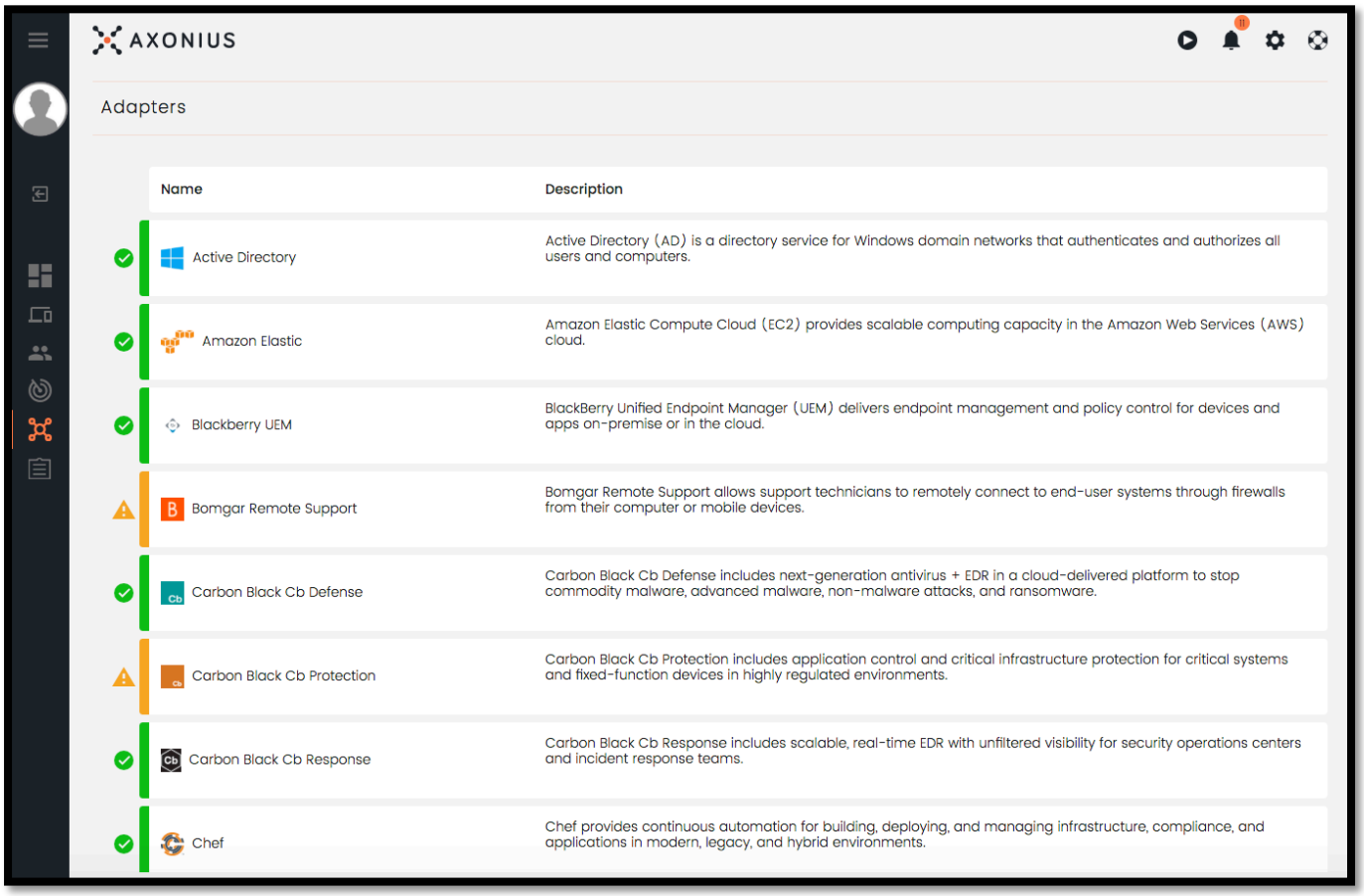
Finally, any security policy on paper is only as good as it is enforced and validated in reality. Implementing a security policy validation process is the only way to make sure that nothing is being missed and that exceptions aren't being exploited.

Cybersecurity Asset Management – The 1st Step to Zero Trust

As mentioned earlier, Cybersecurity Asset Management is a new approach to providing comprehensive visibility into all devices, users, and the security products that cover them in order to validate security policies.

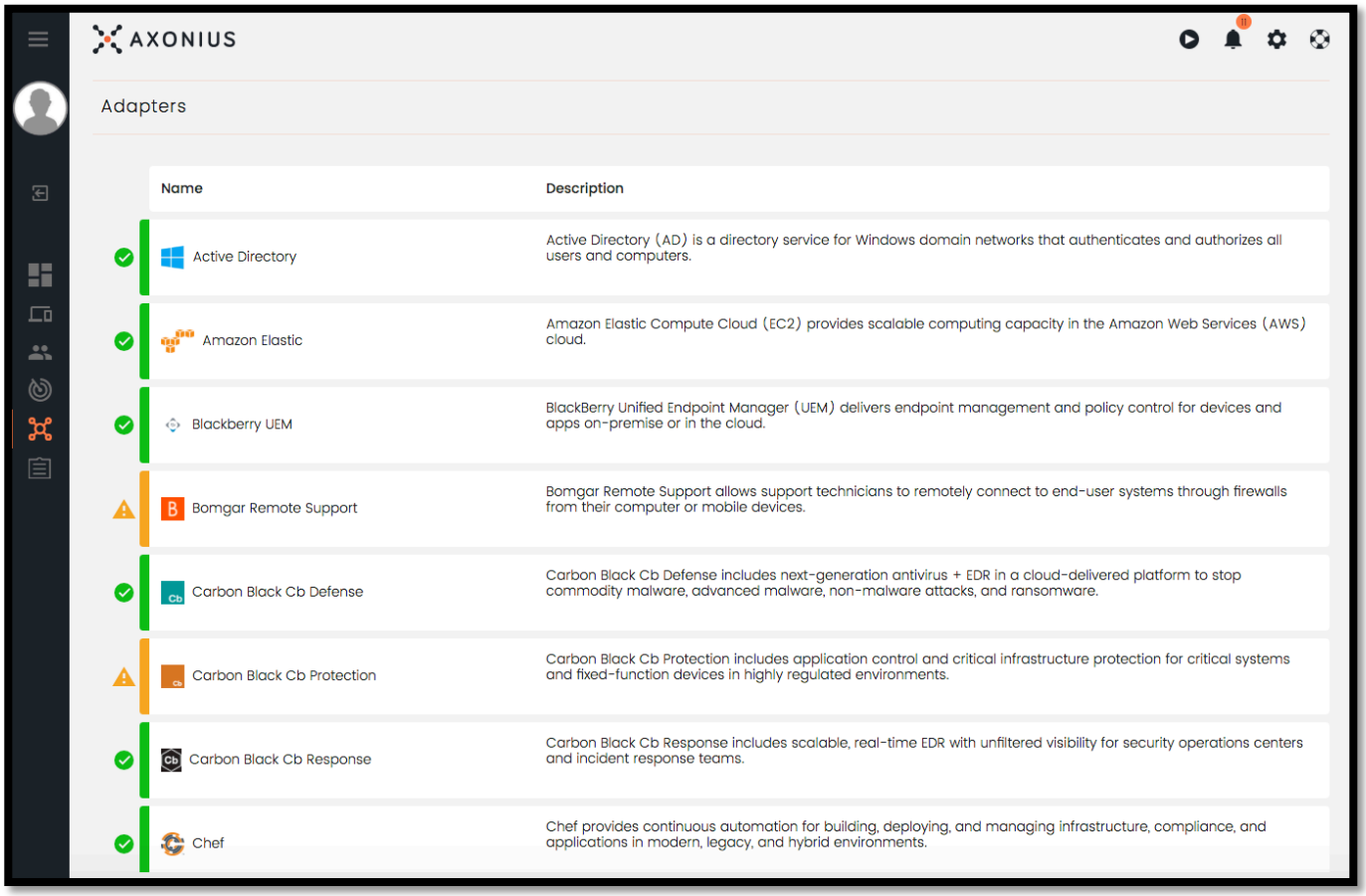
CONNECTING TO EXISTING SECURITY AND IT MANAGEMENT SOLUTIONS

Instead of installing an agent, scanning, or sniffing traffic, Cybersecurity Asset Management solutions connect to the different security and management solutions a customer already uses via adapters. Customers simply provide credentials (API keys, Tokens, etc.), and the system immediately starts collecting and correlating information about assets. This way, there are no agents to install or maintain, no bottlenecks to route traffic through, and there is no limit to scale and no performance degradation.



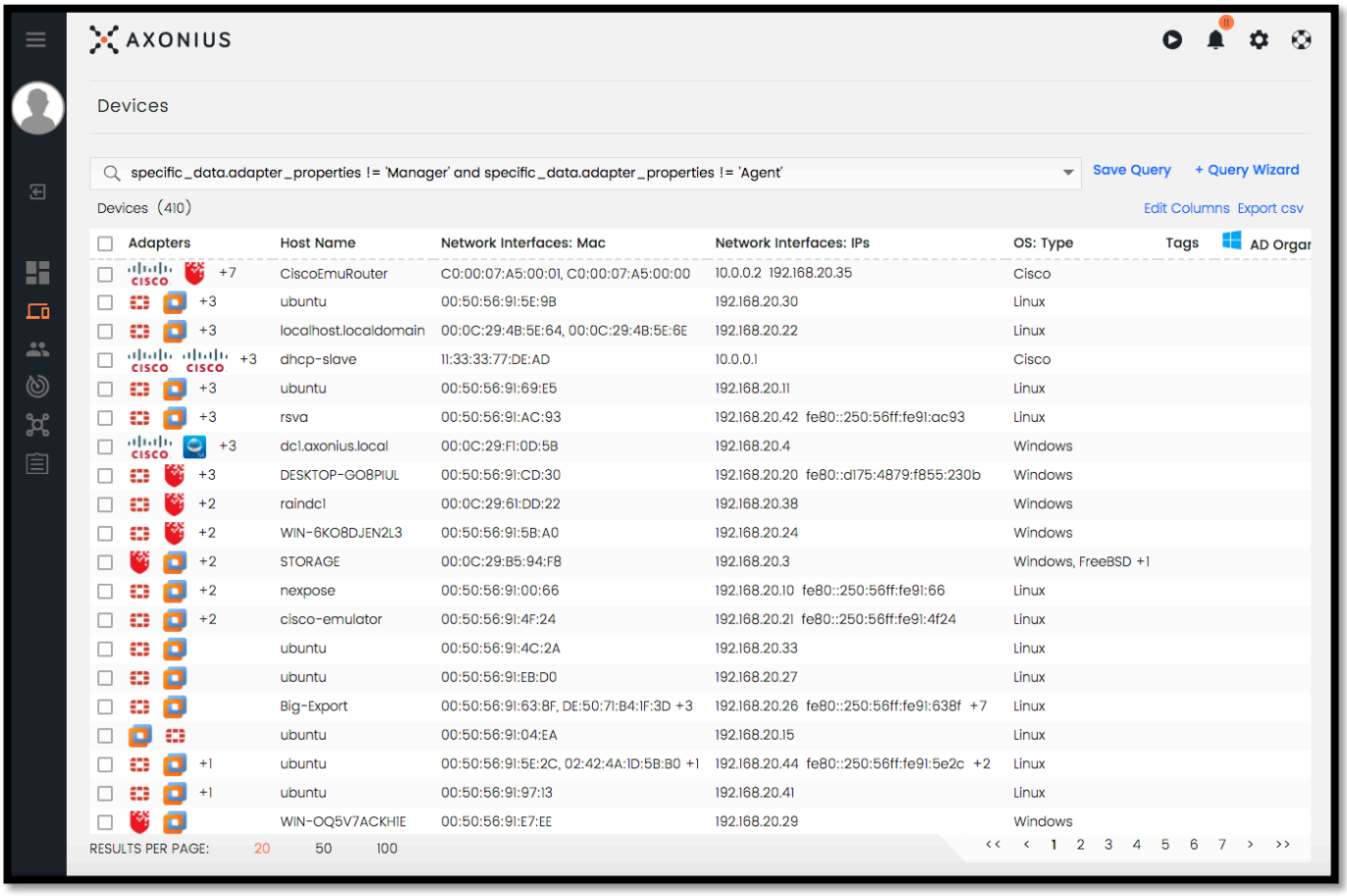
CREATING A COMPREHENSIVE VIEW OF ALL DEVICES

After connecting all relevant adapters, a Cybersecurity Asset Management Platform will create a correlated list of all devices that can be filtered and sorted by any property. As the solution is constantly requesting up-to-date data from every connected solution, the list of devices is always as close to real-time as the connected solutions allow.



IDENTIFYING UNMANAGED DEVICES

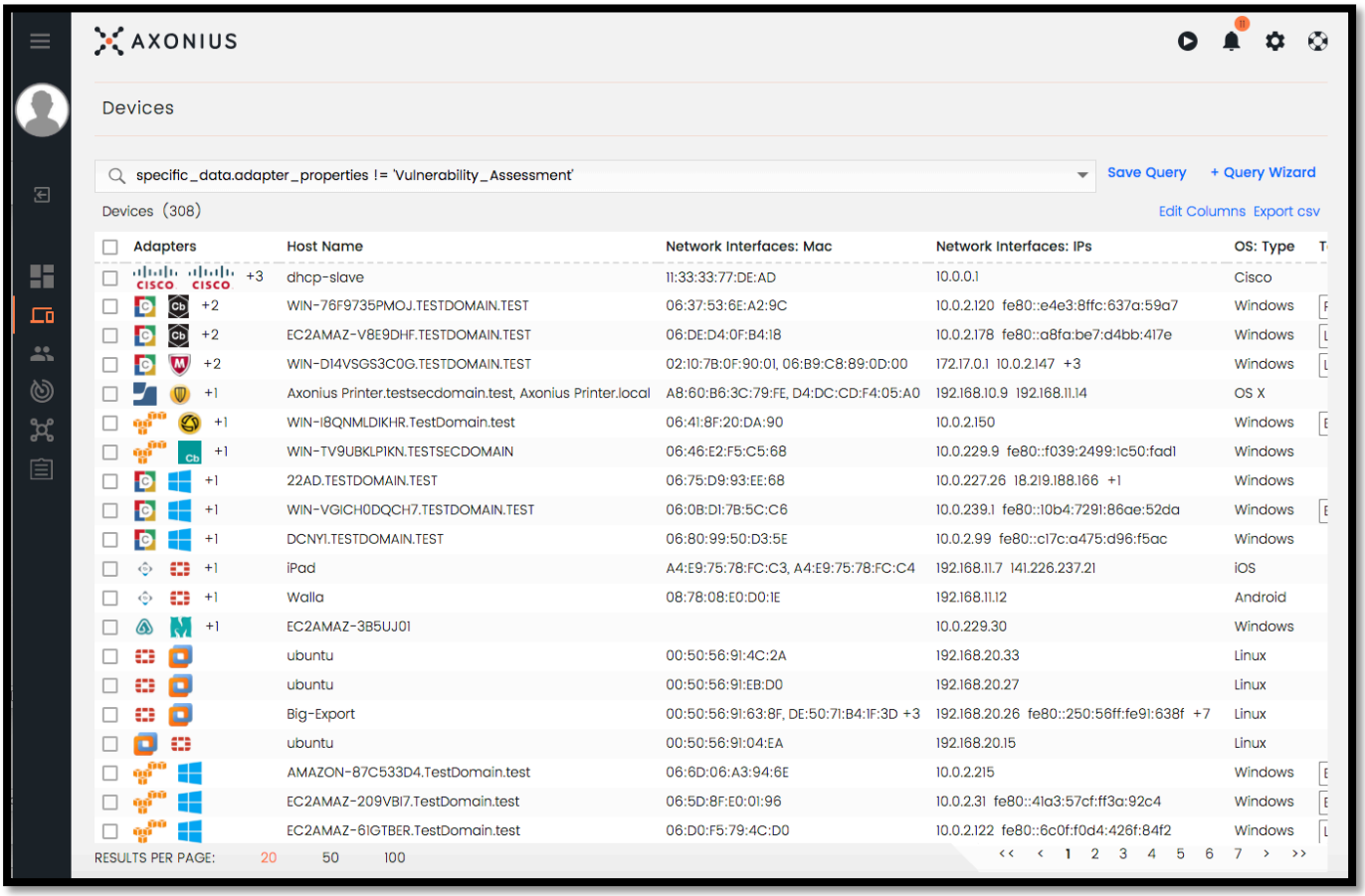
By connecting to the security and management solutions and comparing results to what is known only to the switches and routers, the CSAM solution is able to produce a list of unmanaged devices, allowing customers to distinguish between devices that should not be managed (think of a Smart TV in a conference room or an Amazon Alexa in the reception area), and an AWS instance that the Security and IT teams don't know about.



Unmanaged devices in the Axonius Cybersecurity Asset Management Platform.

UNDERSTANDING SECURITY SOLUTION COVERAGE

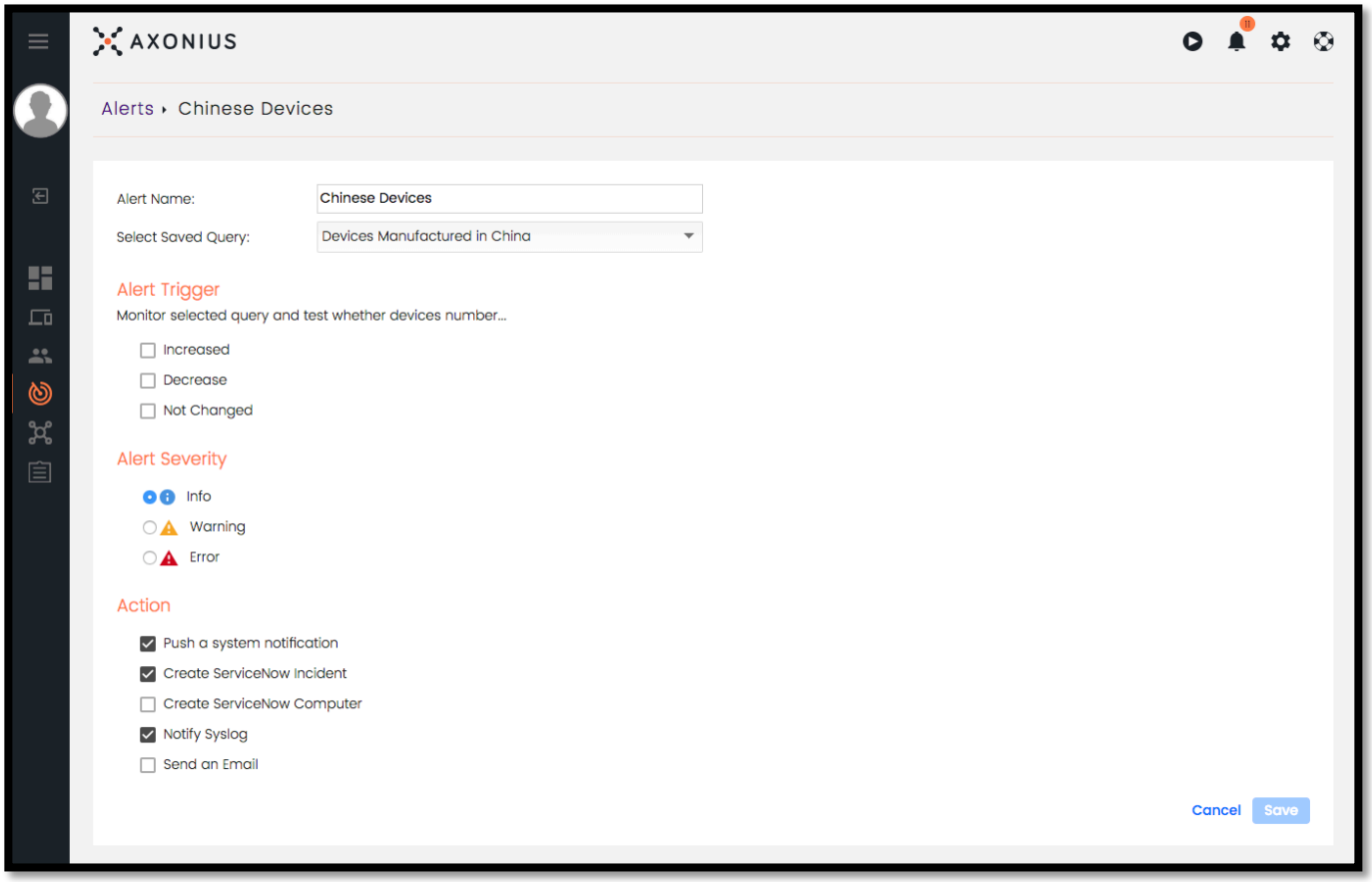
Even with a security policy that dictates every device needs an endpoint agent and must be scanned by a VA tool, most organizations have gaps in coverage. With a CSAM solution, customers are able to understand which devices are not covered so they can act.



Devices not scanned by a Vulnerability Assessment Tool.

CREATING ALERTS

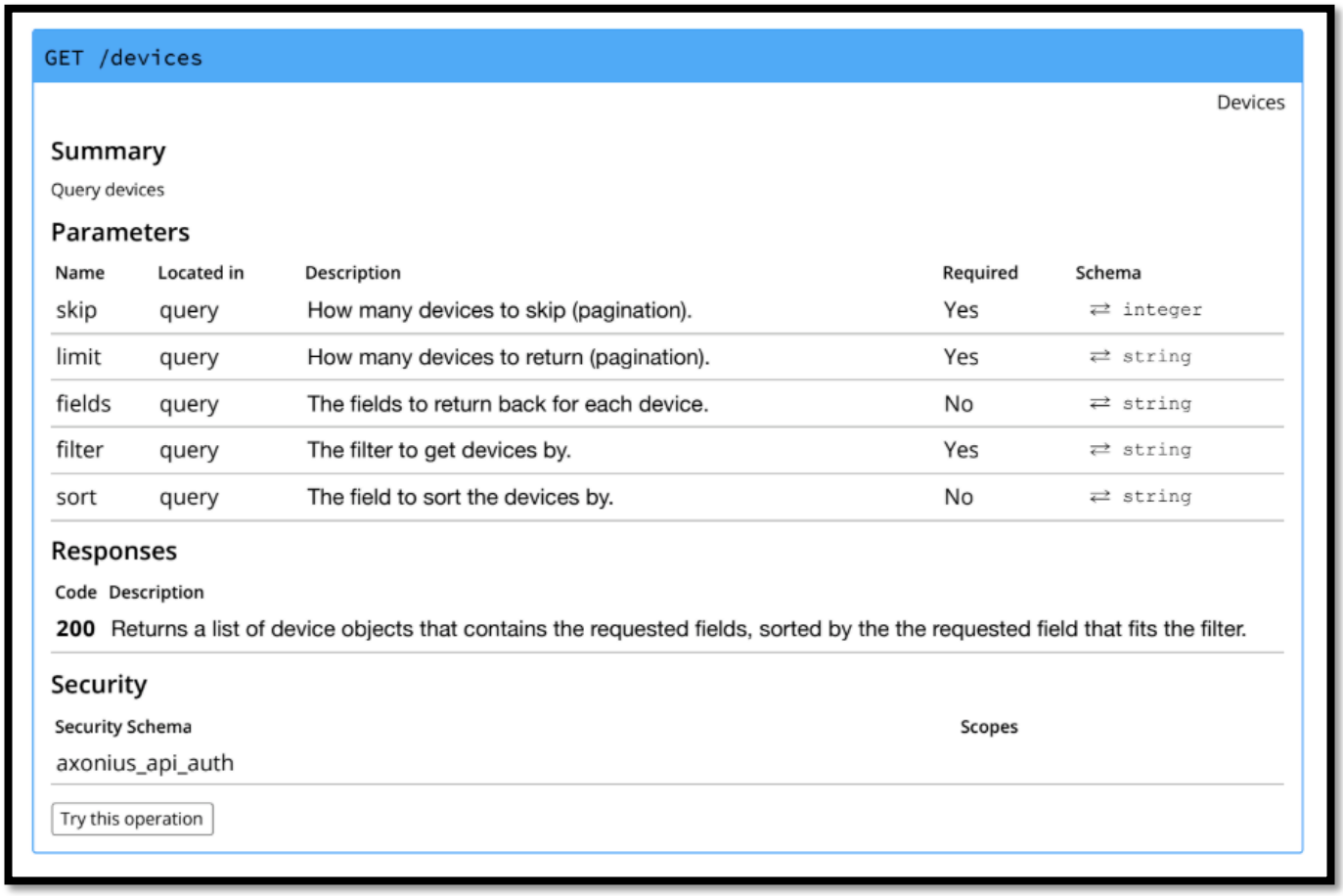
The core value of Cybersecurity Asset Management Tools is the ability to ask questions that validate a security policy in an ongoing basis and to create alerts to notify staff or other solutions when something does not adhere to the policy. To do that, CSAM solutions allow customers to save any query and to create an alert from a query that can be sent via email, syslog, or through an integration with another system (examples include SIEM solutions and ticketing systems).



Example of an alert in the Axonius Cybersecurity Asset Management Platform.

ENHANCING DEVICE AND USER DATA

In many cases, organizations are already using many different security solutions and do not want yet another system to maintain and staff, but instead want to integrate CSAM data with a system of record. Using the API of the CSAM solution, customers are able to extract additional contextual information about users and devices and push that data into their existing systems.



GET /devices

Devices

Summary

Query devices

Parameters

Name	Located in	Description	Required	Schema
skip	query	How many devices to skip (pagination).	Yes	⇄ integer
limit	query	How many devices to return (pagination).	Yes	⇄ string
fields	query	The fields to return back for each device.	No	⇄ string
filter	query	The filter to get devices by.	Yes	⇄ string
sort	query	The field to sort the devices by.	No	⇄ string

Responses

Code	Description
200	Returns a list of device objects that contains the requested fields, sorted by the the requested field that fits the filter.

Security

Security Schema	Scopes
axonius_api_auth	

Try this operation

Sample API calls from the Axonius Cybersecurity Asset Management Platform.

About Axonius

For organizations that see opportunity in today's always-on and always-connected reality, Axonius is the Cyber Security Asset Management (CSAM) platform that lets IT and Security teams see devices for what they are in order to manage and secure all. By easily integrating with customers' existing management and security technologies and using an extensible plugin infrastructure to add custom logic, customers are able to get a unified view of all devices – both known and unknown. Axonius aims to be IT's favorite Security tool and Security's favorite IT tool. For more information and to see what's possible with a universal view of all devices, visit Axonius.com.

Get Started

Because it integrates natively with the Security and IT solutions customers already have, getting started is painless and fast. To get a demo and to see what you can do with a unified view of all assets, click the button below.

Try It Now.

Support and Questions

We are committed to helping our customers deploy, configure, and start seeing value immediately. The POC deployment process will be hands-on, with any and all support services available to get up and running. Should you have any questions, concerns, or product feedback, please do not hesitate to contact your Axonius account representative at any time.

Thank You

Finally, we want to thank you for considering working with Axonius. As IT and Security professionals ourselves, we understand the time and effort it takes to consider a new product. Thank you for trusting us to help you.

Sources Cited

BeyondCorp - A New Approach to Enterprise security
By Rory Ward and Betsy Beyer
December, 2014
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf

What is Zero Trust? A model for more effective security
By Mary K. Pratt
January, 2018
https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html

Salted Hash Video: Learn what the 'zero trust' security model really means
By Steve Ragan and Wendy Nather
https://www.idg.tv/video/87016/learn-what-the-zero-trust-security-model-really-means-salted-hash-ep-29