Remove Roadblocks to Zero Trust with Cybersecurity Asset Management

Cybersecurity in the federal government today is reactive and tactical. It's filled with activities such as reviewing and closing out alerts in a security information and event management (SIEM) system, searching for indicators of compromise from a breach, or conducting incident response investigations. But a seismic shift is occurring as agencies move toward a proactive approach in which they trust nothing and verify everything.

The mindset required for Zero Trust is especially well understood in the defense and intelligence communities when ensuring physical security. Applied to information security, the approach is now a major focus across the federal government as agencies grapple with increasing numbers and severity of cybersecurity attacks, and facilitate remote work for a majority of employees.

In its simplest form, Zero Trust means "trust nothing; verify everything." Users are no longer trusted just because they are authorized on the network. Devices are no longer trusted simply because they are agency-owned. Each device, user, and connection to a network, application, or data is evaluated at the time an action is attempted, then either authorized or declined. It's an entirely different approach to cybersecurity. To achieve this technical shift, a shift in mindset is also required – from the top levels of the agency to each end user.

This mindset change was underway before the COVID-19 pandemic, with about 25% of federal employees authorized to work remotely. Then, in March 2020, that number grew to about 75% teleworking, in a dramatic acceleration of acceptance that government work can be accomplished from almost anywhere.

At the Department of Defense (DoD), Zero Trust is a key follow up to the department's success with widespread telework during the coronavirus pandemic, as **noted by acting DoD CIO John Sherman.**

"But there is more we need to do" to implement Zero Trust security concepts, including undertaking a "philosophical shift" about security, he noted. "This is going to take a whole team effort to make this work," Sherman said, while pledging. "We are going to be a leader for federal colleagues" in showing the way to Zero Trust implementation.

It's a challenge of imagination as IT leaders and agency executives consider how to move from their current state to a future, Zero Trust state. Today, end users may connect to the agency network via a VPN, while some may still enter a building to access a system. They're granted access based on where they are and how they are connecting. In the future Zero Trust state, access decisions will be much more granular. Getting to Zero Trust can be a daunting journey, and existing guidance can seem abstract and overwhelming.

Once an agency establishes its vision for Zero Trust and begins to shift the collective mindset to "never trust, always verify," a series of tactical steps can ease the Zero Trust journey by breaking it down into manageable, incremental components.

Step 1: *Asset Management*

Asset management is foundational to cybersecurity. Agencies need a comprehensive inventory of all hardware, software, and network assets. This inventory must include data on the software running on all machines, so agencies can ensure that all assets are running licensed and patched applications.

Without an accurate understanding of everything in the agency environment, all other initiatives suffer. But traditional approaches to compiling an asset inventory are manual and error-prone. They're time consuming and can quickly become obsolete.

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

Step 2: *User Identity Management*

Because end users are no longer trusted based solely on their presence on the agency network, agencies need a new way to determine if end users should be allowed to access an application or data, or take other actions on agency systems.

In most cases, the answer is to validate the user identity. Today, most large enterprises have identity information sprinkled throughout user directories. They need a way to efficiently manage user identities in one place. The solution is centralized identity and access management with Security Assertion Markup Language-based single sign-on (SSO).

For a quick win on the way to Zero Trust, agencies can determine which applications can be easily incorporated in an SSO solution. The web browser provides the secure connection, and the SSO solution authenticates the end user, eliminating the need for a VPN. This solution means the network is no longer trusted – a major step toward Zero Trust.

Step 3: *Endpoint Security*

Because the network is no longer trusted, users can be anywhere. To enable anywhere access, agencies need to verify the security of users' devices and network connections.

To do this, agencies can integrate the SSO solution with their mobile device management (MDM) or endpoint management solution. Then, when the access decision is made, it's based not only on the user identity, but also on whether the device is in a trustworthy state.

Agencies may be well on their way toward Zero Trust, having taken one or more of these steps already. The journey is unique to each organization, and like any other major technology initiative, an incremental approach is key to success. That incremental approach begins with quick win projects that enable the agency to gain allies for the Zero Trust movement.

Why Zero Trust?

The cybersecurity benefits of Zero Trust are clear. A proactive approach to security reduces the chance of a cyberattack and makes more time for tactical response if a breach occurs.

Zero Trust is also gaining momentum because it enables a better user experience. Too often, security gets in the way of the user. But Zero Trust eliminates clunky VPN clients that authenticate with a proprietary mechanism. Instead, Zero Trust incorporates the authentication mechanism seamlessly into the applications and systems that end users access regularly. And with SSO, end users have fewer credentials to remember. As a result, Zero Trust provides the same ease of access and user-friendly functionality that end users enjoy in their personal use of applications and services. Security only gets in the way if end users try to do something they're not authorized to do.

Zero Trust also brings tangible benefits to IT operations:

- Centralizing user identities into a single or fewer identity stores means fewer identity directories to manage
- Implementing SSO reduces the time and cost associated with user provisioning and deprovisioning, and frees time for higher-level IT management and cybersecurity work
- Creating new opportunities to securely deploy cloud-based applications to meet evolving mission requirements

Axonius Enables the Move to Zero Trust

To get to Zero Trust, agencies must understand who is accessing agency IT resources, what devices they are using, and whether those people and devices are in a secure, trustworthy state. Historically, many organizations gained this information via network access control (NAC) tools. For some legacy and highly sensitive applications that continue to operate and need on-premises access, NAC and internal network vulnerability scans will continue to be important sources of information.

But when end users are allowed to connect to agency resources from outside the agency network, agencies must tap into additional data sources, such as the SSO solution, MDM tool, and systems management tool, and then make sense of the data.

Axonius is a cybersecurity asset management platform that enables agencies to bring all of this information into a single view. It enables agencies to:

- Gather data from any source that provides detailed information about assets
- Correlate and deduplicate that data to generate a view of every asset and what's on it
- Continually validate every asset's adherence to the overall security policy
- Create automatic, triggered actions whenever an asset deviates from security policy

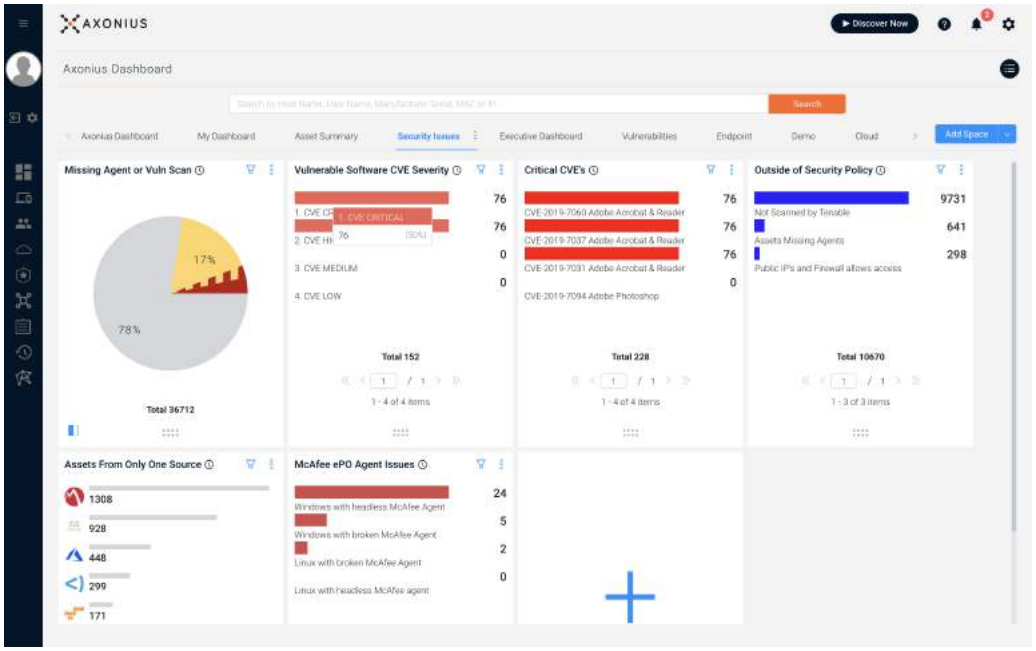
Potholes to Avoid on the Road to Zero Trust

Splintered user idenitity: Incorporate SSO whenever possible. Without SSO, end users get prompted to log in again and again. Security gets in the way of a seamless user experience.

Unrealized expectations: Ensure end users understand what they are allowed to do (and not to do) on agency networks and in agency applications. For example, communicate policies around actions that can be taken with personal devices or mobile phonts vs. agency laptops and desktios. If access parameseters are well understood, end users are less likely to be denied access – and if they are, end users will understand why.

Gaps in expertise: Agencies may need to hire or retain personnel to implement and manage the technnologoies that enable zero trust.

Axonius enables agencies to rapidly identify and address security coverage gaps. For example, agencies can easily understand which systems don't have the agency's endpoint security agent and act to remedy that gap.



While implementing Zero Trust is a heavy lift upfront, it gives network defenders more opportunities to identify threats and more time to remediate incidents.

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 on 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

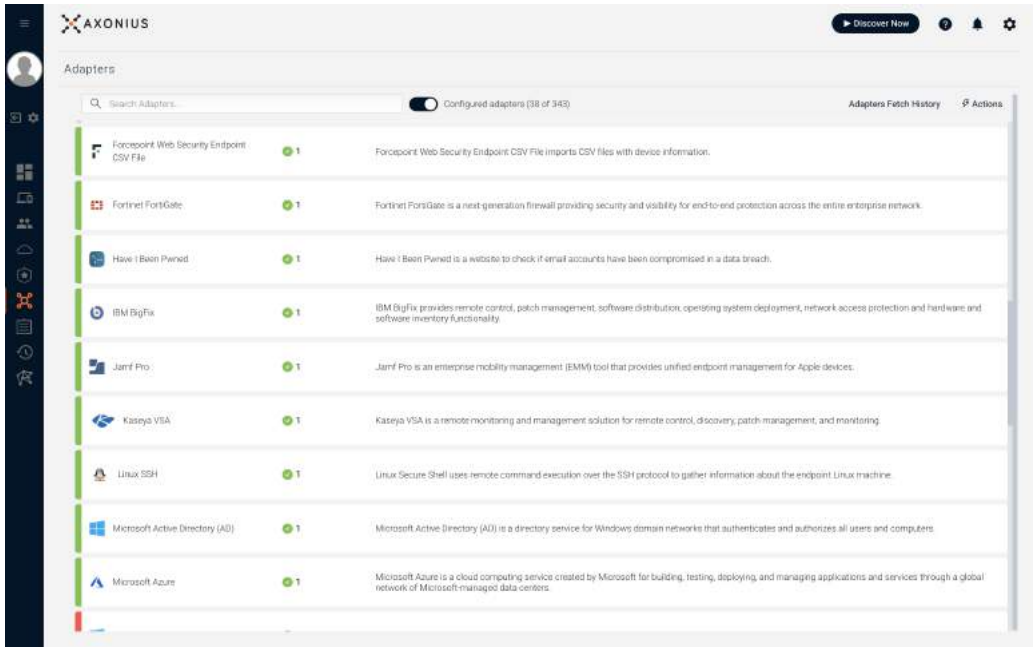
Finally, any security policy on paper is only as good as it is enforced and validated in reality. Implementing a security policy validation process is the only way to make sure that nothing is being missed and that exceptions aren't being exploited.

Getting Started with Cybersecurity Asset Management for Zero Trust

As mentioned earlier, cybersecurity asset management (CSAM) 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's no limit to scale and no performance degradation.



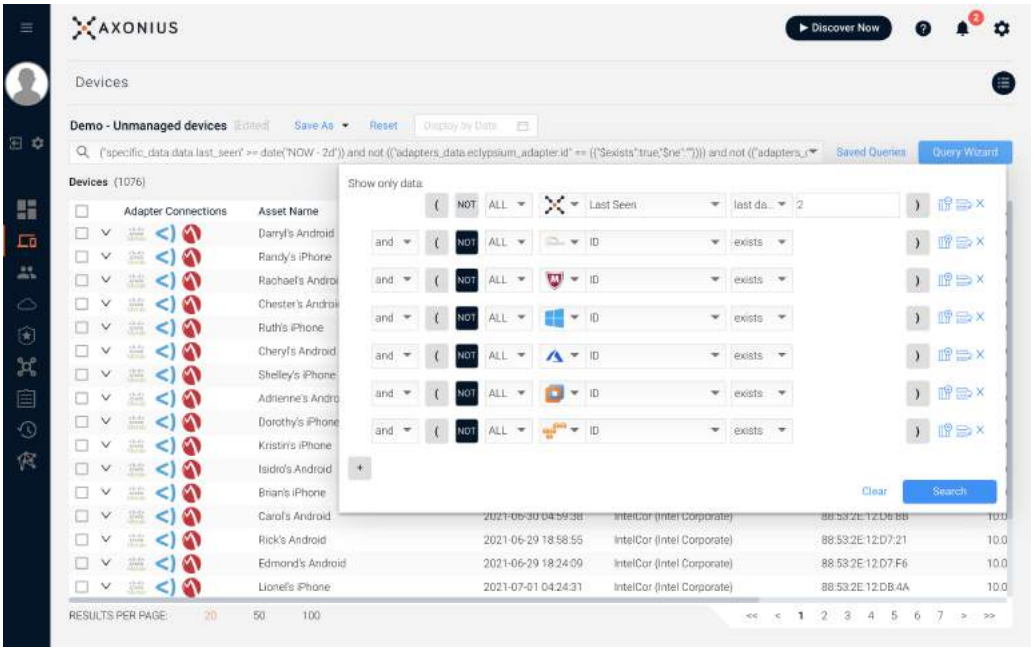
CREATING A COMPREHENSIVE VIEW OF ALL DEVICES

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.

Total Devices Seen	200692 (203083)
Axonius Device Correlation	▼
Total Unique Devices	40363

IDENTIFYING UNMANAGED DEVICES

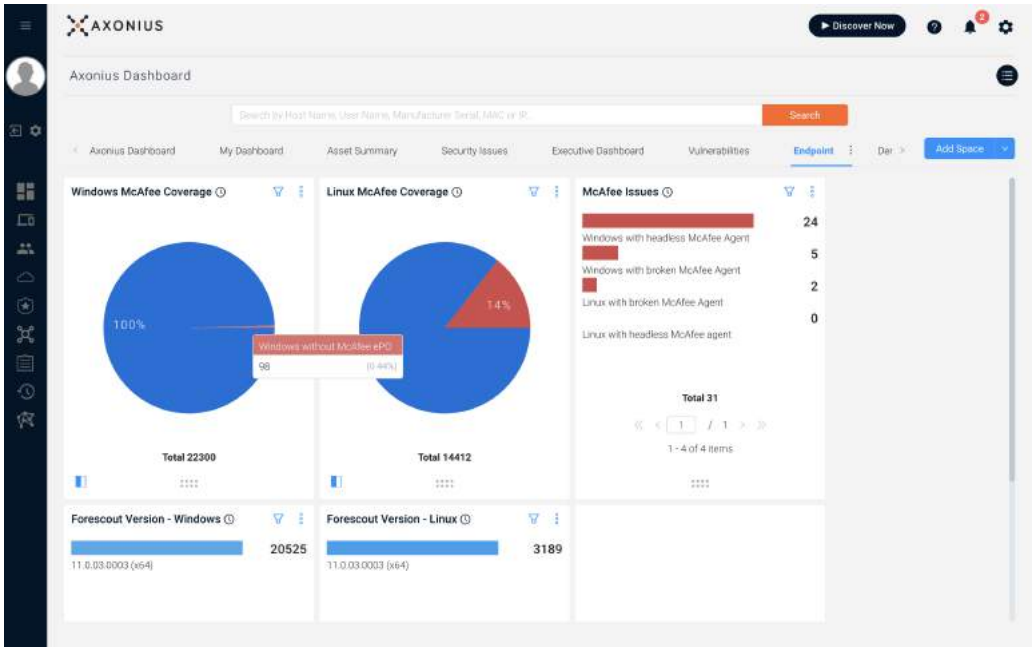
By connecting to the security and management solutions, and comparing results to what's known only to the switches and routers, the CSAM solution is able to produce a list of unmanaged devices, allowing customers to distinguish between devices that should not be managed (think of a smart TV in a conference 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

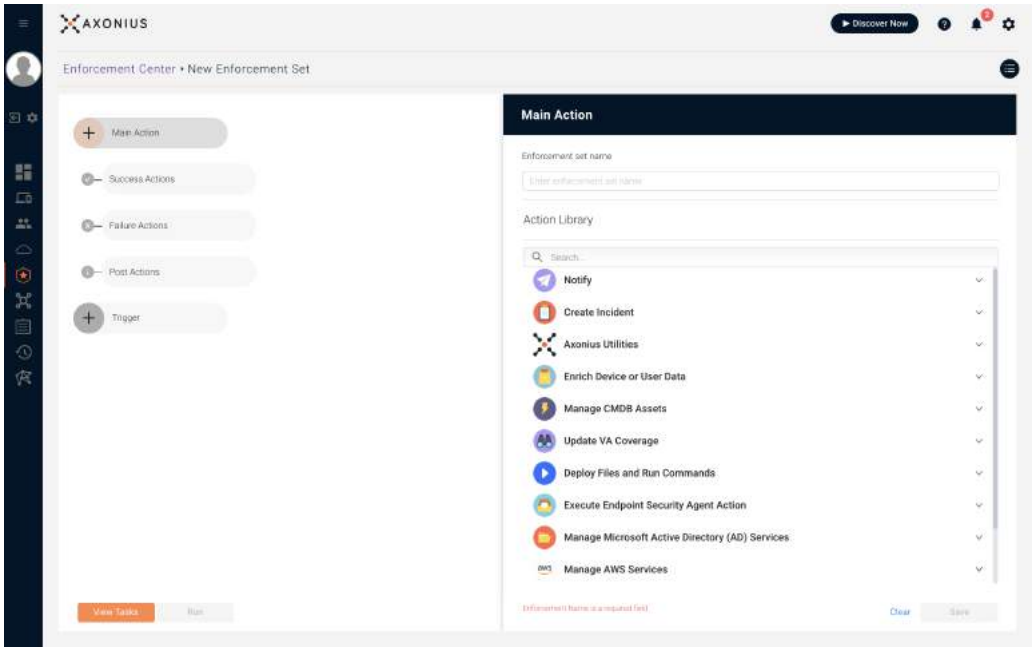
Even with a security policy that dictates every device needs an endpoint agent and must be scanned by a VA tool, most organizations have gaps in coverage. With a CSAM solution, customers are able to understand which devices are not covered so they can act.



Charts Displaying Endpoint and NAC Coverage

ENFORCING POLICIES

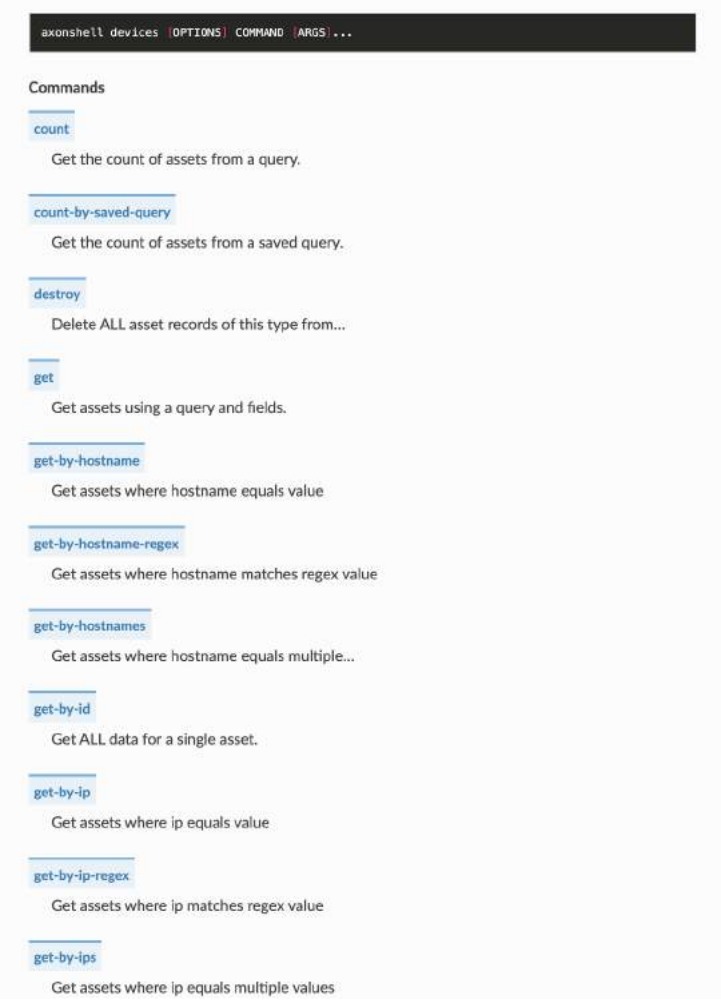
The core value of cybersecurity asset management tools is the ability to ask questions that validate a security policy on an ongoing basis and to create custom response actions and notify teams when something does not adhere to the policy. To do that, CSAM solutions allow customers to program custom actions using saved queries, or create ad hoc enforcement actions. Actions include simple alerts and notifications, creation of helpdesk tickets, device and user enrichment, or direct actions to change the configuration of devices and users.



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 don't 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.



Sample API calls from the Axonius Cybersecurity Asset Management Platform.

GET STARTED WITH AXONIUS FEDERAL SYSTEMS

Axonius is uniquely positioned to deliver a comprehensive view of all IT assets, users, and software. Gain an always-up-to-date single source of truth about your environment. To learn more, visit **axoniusfederalsystems.com**