MeriTalk®
Improving the Outcomes
of Government IT

AXONIUS

REMOVE ROADBLOCKS TO ZERO TRUST WITH CYBERSECURITY ASSET MANAGEMENT

Cybersecurity in the Federal government today is reactive and tactical, filled with activities such as reviewing and closing out alerts in a security information and event management 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 percent of Federal employees authorized to work remotely. Then, in March 2020, that number grew to about 75 percent teleworking, in a dramatic acceleration of acceptance that government work can be accomplished from almost anywhere.

At the Department of Defense, zero trust is a key follow-up to the department's success with widespread telework during the coronavirus pandemic, noted acting 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; some may still enter a building to access a system. They are granted access based on where they are and how they are connecting. In the future, zero trust state, access decisions are 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, however, 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 One

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 Two

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 Three

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.

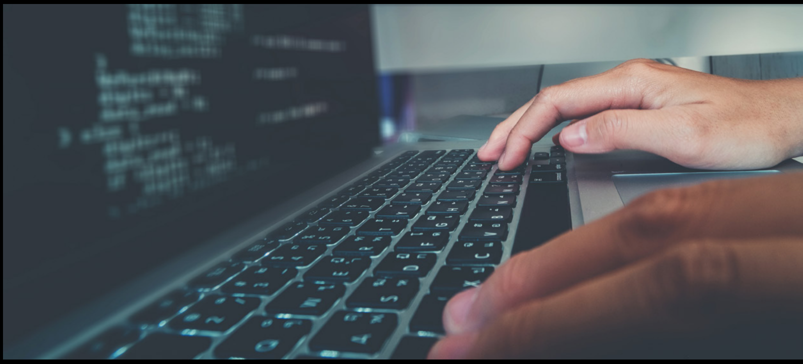
To do this, agencies can integrate the SSO solution with their mobile device management (MDM) or endpoint management solution. Then, when the access decision is made, it is based not only on the user identity, but also on whether the device is in a trustworthy state.

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

Agencies are paying for other services to enable zero trust, of course, but ultimately, costs will be lower because more activities are automated, which increases the efficiency and scalability of IT resources.

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 be accessed on premises, 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

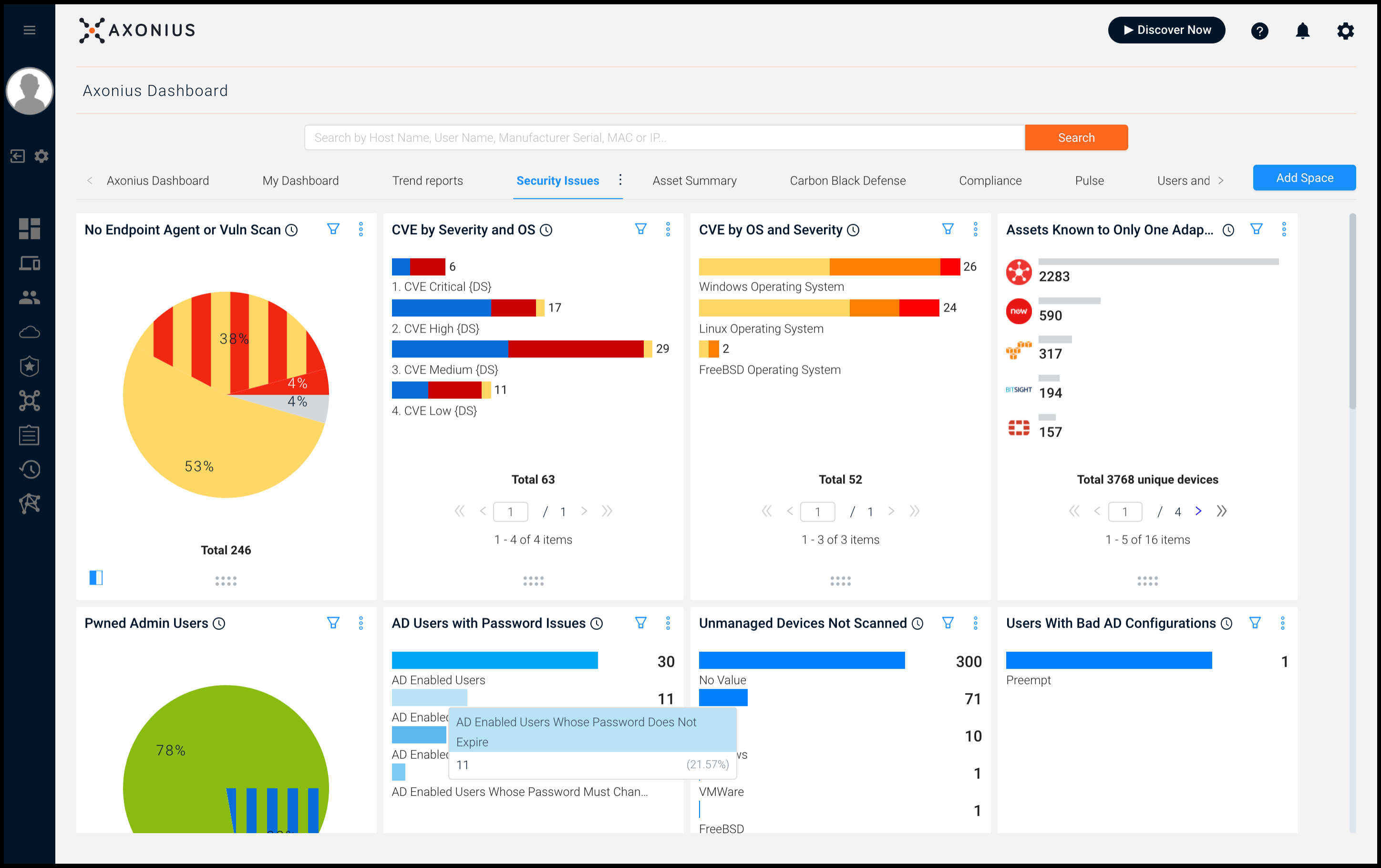
Potholes to Avoid on the Road to Zero Trust

Splintered user identity. 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 do) on agency networks and in agency applications. For example, communicate policies around actions that can be taken with personal devices or mobile phones vs. agency laptops and desktops. If access parameters 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 retrain personnel to implement and manage the technologies 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 up front, it gives network defenders more opportunities to identify threats and more time to remediate incidents.

How can Axonius help? **SEE FOR YOURSELF**

MeriTalk®
Improving the Outcomes of Government IT

AXONIUS