THE ROAD TO ZERO TRUST FOR FEDERAL AGENCIES

AXONIUS FEDERAL

Cybersecurity in the federal government today is reactive and tactical, but more agencies are starting to prioritize a proactive approach in which they embrace the core principles of Zero Trust security: trust nothing and verify everything. Since organizations are faced with an increasing amount of cyber attacks that are higher in severity and CISA guidelines are steering agencies towards the Zero Trust Maturity Model, leaders are adopting a Zero Trust mindset towards cybersecurity that is especially well understood in the defense and intelligence communities.

Why are federal leaders choosing the Zero Trust security approach?

A proactive Zero Trust approach means that users are no longer trusted because they are authorized on a network and are instead evaluated after any action is attempted and then either authorized or declined. Here's why federal agencies are following this framework.

Zero Trust gives federal security teams an advantage:

- Reducing the chance of a cyber attack makes more time for tactical response when a breach occurs.
- Teams enable a better user experience by eliminating clunky VPN clients, and instead seamlessly authenticate into applications and systems end users regularly use, improving access and functionality.

Zero Trust provides tangible benefits to federal IT operations:

- Centralizing user identities into single or fewer identity stores leads to fewer identity directories to manage.
- Implementing SSO capabilities reduces the time and cost associated with user provisioning and deprovisioning, freeing time for higher-level IT management and cybersecurity tasks.
- Zero Trust creates opportunities to securely deploy cloud-based apps that meet evolving mission requirements.

How can federal agencies shift towards a Zero Trust mindset?

The following three steps help IT and security leaders move from their current state to a future, Zero Trust state:

ASSET MANAGEMENT:

Asset management gives agencies a comprehensive inventory of all hardware, software, and other network assets necessary to gain an accurate understanding of what's already in their tech stack and whether or not all applications are licensed and patched. Cybersecurity asset management platforms automatically give you full visibility into your asset inventory (which was once a manual and error-prone process) and then validate compliance and automate remediation.

USER IDENTITY MANAGEMENT:

Zero Trust practices mean that users are no longer trusted based solely on being on the network. So, agencies validate the user identity before allowing access. Large organizations need a way to manage user identities in one location – the solution is centralized identity and access management. For a quick win on the way to Zero Trust, you can determine what apps can be easily incorporated into a single sign-on (SSO) solution, eliminating the need for a potentially costly VPN.

ENDPOINT SECURITY:

Because the network is no longer trusted, users can be anywhere. To enable anywhere access, the security of users' devices and network connections must be verified. This can be done by integrating the SSO solution with a mobile device management (MDM) or endpoint management solution. Then, when access decisions are made, they are based not only on user identity but also on whether the state of the device is trustworthy.

Federal agencies may have already taken some of these steps, and each journey to Zero Trust is unique. The key to success is approaching these changes incrementally.

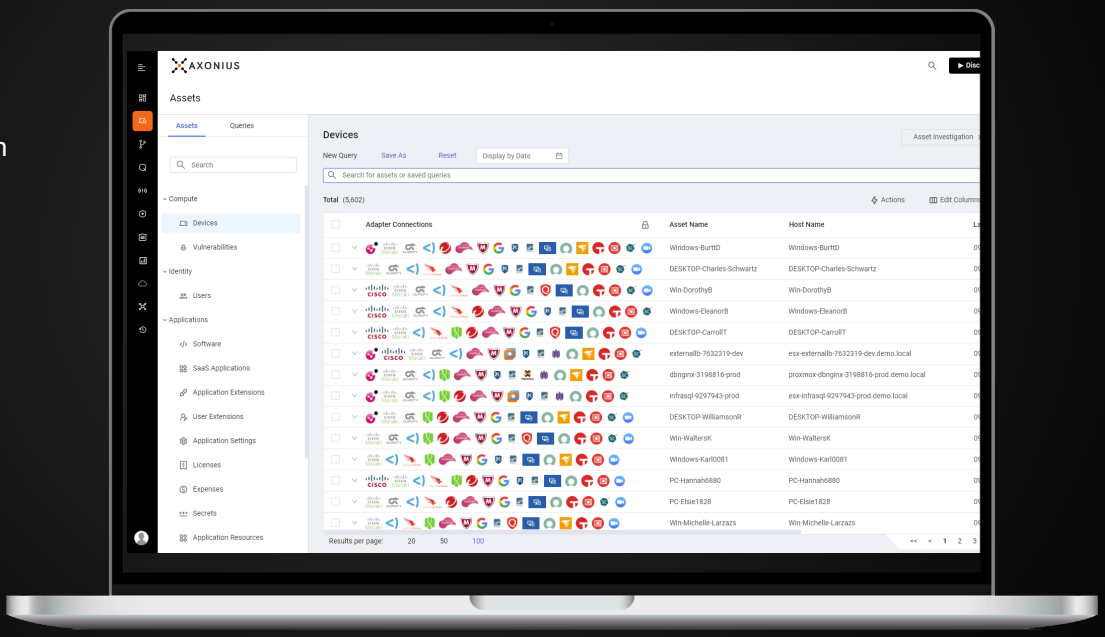
How Axonius Federal Systems helps federal agencies achieve Zero Trust

AXONIUS FEDERAL

As you move towards a Zero Trust model, NAC and internal network vulnerability scans will continue to be important sources of information for legacy applications that likely still need on-prem access. But as end users connect outside the network, federal 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. The Department of Defense includes securing users and devices in its Zero Trust strategy plan – which solutions like the unified Axonius Platform help you achieve by increasing visibility into the security state of the assets your agency already has.

Axonius enables agencies to bring all of this information into a single view and:

- 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



Shifting from a traditional perimeter-based approach to Zero Trust is not an all-or-nothing process. By approaching Zero Trust as an aspirational future state and by choosing the right asset management platform, federal agencies can take gradual steps with the goal of achieving Zero Trust in mind.

Interested in seeing what Axonius Federal Systems can do for your organization?

LET'S TALK