Quest
Public Sector

Securing the federal government

Work with the proven leader in identity-centric cybersecurity and recovery management

Quest Public Sector is an established leader in identity-centric cybersecurity, including Zero Trust implementations, identity governance and Active Directory (AD) management. We are an expert in Zero Trust centric Active Directory lifecycle management for the federal government. Read on to see how we can help fast track Zero Trust deployment by leveraging your existing Active Directory infrastructure.

We are a federal-focused solution provider to over 90 percent of the U.S. government across civilian and defense agencies, and the intelligence community.

Active Directory (AD) is the core of the modern identity infrastructure

With more than 95 percent of federal agencies centered on Active Directory for authentication and authorization, it plays a crucial role in your cybersecurity strategy, including implementing Zero Trust principles across your enterprise.

Zero Trust is easily achievable

For many federal agencies, Zero Trust is well within reach when they rely on modular and integrated solutions, including Privileged Access Management (PAM), Active Directory (AD)/Azure AD management, event log data collection, and identity governance and administration (IGA). This integrated approach satisfies the core tenets of Zero Trust security while delivering an optimal end-user experience.

WHAT IF your agency could:

- Recover Active Directory at the click of a button?
- Provision user permissions down to the attribute level in Active Directory?
- See every change to Active Directory in real-time?
- Protect critical Active Directory groups and accounts from unsolicited changes?
- Govern the identity lifecycle from beginning to end?
- Implement a Zero Trust cybersecurity model in weeks instead of months (or years)?

95% of Fortune 1000 rely on Active Directory (AD) and Azure AD

95M Active Directory accounts are attacked daily

Why Zero Trust?

- Comprehensive identity lifecycle management for a secure and compliant environment
- Expand to identity governance and administration (IGA)
- Protect tier 0 Active Directory: delegate permissions, prevent changes
- Real-time Active Directory monitoring
- Consolidate domains to reduce cost, overhead, and threat surface
- Automate Active Directory recovery from malicious activity
- Surpass native management tool limitations
- Ensure the right people have the right access to the right resources at the right time

User-identity security

Our identity solutions enhance the management of Active Directory and protect against intrusions.

Privileged access

Additionally, our advanced identity solutions manage privileged access, ensuring that only verified users can access sensitive data and privileged resources. Your agency can benefit from the robust protection measures that our solutions offer.

Data and system recovery

Plus, if there is a breach or a systems failure, we offer market leading recovery solutions.

Enhanced Microsoft and Active Directory environment governance

Our state-of-the-art tools enable effective governance in intricate Active Directory environments. As a leading provider of enterprise-grade directory service management, we empower operators to maintain identity security as a part of a Zero Trust environment.

Our identity-centric approach to cybersecurity allows agencies to implement Zero Trust and least-privilege security models effectively.

Protect

Delegate granular permissions to ensure Active Directory is secure

Monitor

Vision into infrastructure and performance tied to analytics

Consolidate

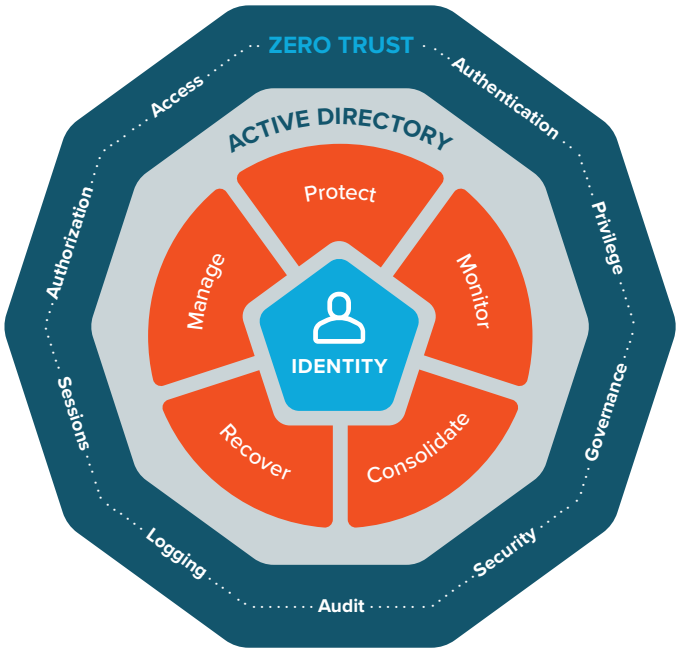
Simplify your IT strategy for enhanced security and performance

Recover

IT resilience enables your agency to bounce back from challenges

Manage

Centralized, secure and integrated administrative tools enable your achievement of a Zero Trust model



Quest Public Sector, 700 King Farm Blvd. Suite 250, Rockville, MD. 20850 | www.questpublicsector.com.

Quest
Public Sector