GovCIO MEDIA & RESEARCH

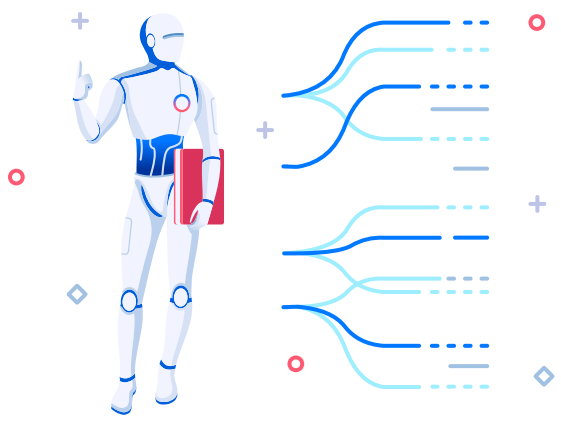
GOV Focus

Navigating Federal Zero Trust Development

Agencies must prioritize strategies to enhance their zero-trust architecture since the White House's zero trust executive order. Experts from the Interior Department and CyberArk discuss their progress and what lies ahead amid shifting priorities.

AI and machine learning are critical in managing the growing number of machine identities, which significantly outnumber human identities

45:1 and rising



Managing machine certificates effectively is essential, especially as certificate lifespans shorten, moving from

3 years to 90 days

Watch for More Insights

Zero-Trust Implementation at DOI

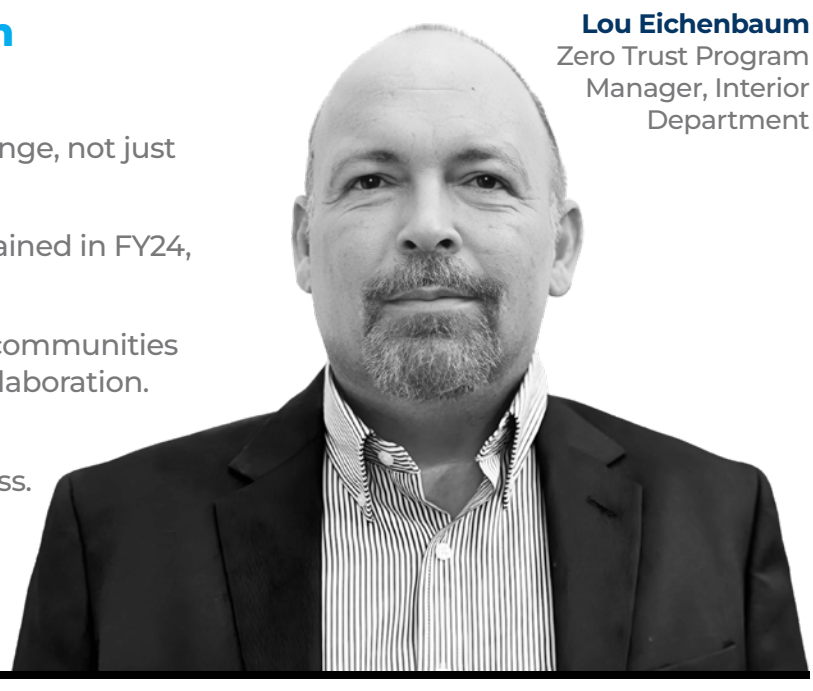
Initial focus spurred by Executive Order 14028 and OMB memo 2209.

Core areas include:

1. **Data Management:** Prioritized categorization and tagging of data.
2. **Identity Management:** Implemented phishing-resistant MFA, increasing adoption from 40% to 92% across applications.
3. **Micro-Segmentation:** Focused on north-south segmentation to mitigate workstation risks, deploying SASE solutions for 70,000 employees.

Cultural Shift & Integration with Customer Experience

- Zero trust is a "people and process" challenge, not just technological.
- Training initiatives: Over 100 employees trained in FY24, aiming for 200 more.
- Built internal and federal-wide zero trust communities of practice for knowledge-sharing and collaboration.
- Zero trust aligns with modern computing environments to simplify and secure access.
- Collaborative efforts with DOI's digital experience officer to balance cybersecurity with user experience.



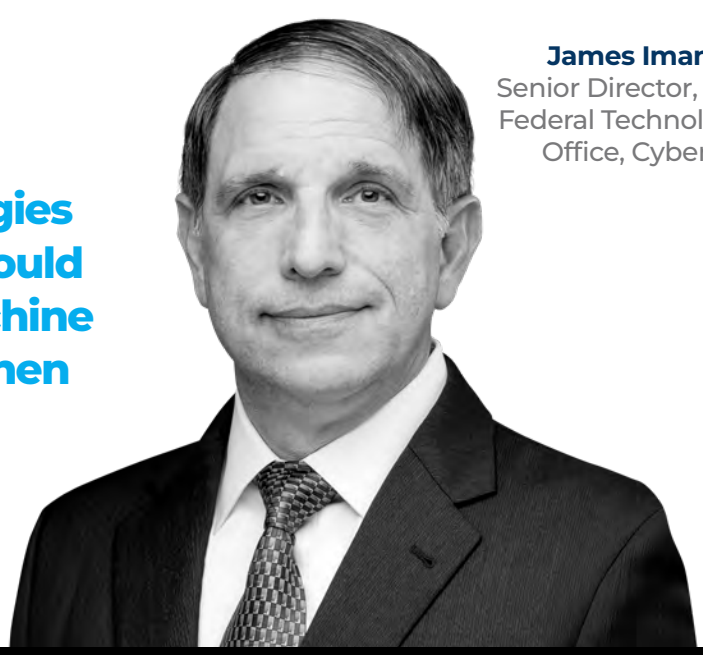
Lou Eichenbaum
Zero Trust Program Manager, Interior Department

Insights on Zero Trust

Encourage the need for agency-wide collaboration beyond just IT or cybersecurity teams. Collaboration ensures alignment with mission-critical objectives while addressing threats. People and processes take precedence over technology in zero-trust frameworks. Zero trust enables secure and efficient access to tools and data by addressing risks with micro-segmentation. Effective implementation involves balancing security goals with agency missions and user needs.

What's Next for Zero Trust in 2025?

> **"We've got to get the technologies and processes in place so we could rapidly both monitor those machine identities and change them when they're needed to ..."**



James Imanian
Senior Director, U.S. Federal Technology Office, CyberArk

Zero Trust Architecture in Emerging Technologies

OPPORTUNITIES:

Enhanced Security:

- **AI & Machine Learning:** Automates threat detection, log analysis and anomaly detection, providing faster responses to security issues.
- **Zero Trust Model:** Automates threat detection and log analysis, providing faster responses to security issues.

Scalability:

- With machine identities outnumbering human identities, AI enables organizations to handle this growth efficiently.
- Automating the management of short-lived machine certificates supports scalability without adding undue manual workload.

Collaboration and Education:

- Breaking silos encourages shared accountability and knowledge across teams, fostering innovation and resilience.
- Training and upskilling IT professionals improves their ability to handle modern cybersecurity challenges.

Operational Efficiency:

- AI reduces manual workloads for IT staff by automating repetitive tasks like log reviews.
- Cross-functional collaboration in zero-trust architecture promotes streamlined communication and integrated decision-making.

CHALLENGES:

Cultural Resistance:

- Transitioning to a zero-trust model requires significant cultural change, which can encounter resistance from staff accustomed to traditional systems.
- Siloed teams, such as application developers, may struggle to adapt to collaborative, security-focused workflows.

Dependence on Technology:

- Over-reliance on AI and automation introduces risks, such as errors in AI models or system failures.
- Managing non-human identities securely requires sophisticated tools, which could be a single point of failure.

Quantum and AI Uncertainty:

- Quantum computing timelines and impacts are still uncertain, making it difficult to plan effectively.
- While AI is powerful, it requires monitoring to avoid issues like false positives in security or inappropriate decision-making.

Cost and Training:

- Implementing advanced technologies like AI, machine learning, and post-quantum encryption is expensive.
- Continuous education and upskilling of staff are necessary but resource intensive.

Watch for More Insights