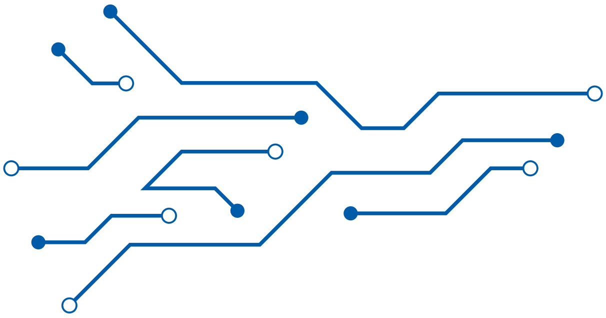
# Federal Perspectives on the Future of Cloud

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Palo Alto Networks, January 2024

Cloud applications are at the center of every digital enterprise, and AI-led development is certain to accelerate innovation. In this digital age, federal agencies must approach cloud security in a way that's intuitive for users and highly effective at reducing risk. In a recent roundtable discussion, federal experts discussed the future of cloud within this advancing technical landscape by sharing the challenges and opportunities facing their agencies.

## Misconceptions and Security Concerns

Agencies are working to overcome persistent misconceptions about data access and security in the cloud. Even with robust infrastructure, vulnerabilities like DNS outages can disrupt data accessibility. Agencies need to build redundant pathways in order to maintain consistent access to their data. Zero Trust architectures are crucial for building trust and mitigating risks.



## Transitioning to the Cloud

The move to the cloud demands a nuanced approach. Agencies need to assess application suitability and maturity levels before migrating. Additionally, workforce training and cultural shifts are essential to embrace the cloud's full potential.

Investment in workforce training and competitive compensation packages are essential to retain skilled personnel and navigate multicloud environments. Agencies find it challenging to find adequate cloud tech support from vendors and contractors. Some agencies have lost dedicated support due to recent tech layoffs in the private sector.

## Optimizing for Efficiency and Scale

Leveraging cloud resources efficiently is another challenge. Optimizing workloads and accurately forecasting financial implications are crucial for responsible stewardship of taxpayer dollars. Furthermore, overcoming the fear of scale is necessary for agencies to fully unleash the cloud's potential.

## Meeting Standards and Simplifying Security

Striking a balance between industry standards and agency-specific security and financial constraints is a delicate act. Vendors must also comply with numerous security standards to work with federal agencies, making the process cumbersome and complex. Simplifying the security landscape, potentially through standardized security models, could alleviate confusion and unlock access to more vendors.

## Security Beyond FEDRAMP

While FEDRAMP offers a valuable baseline, comprehensive security requires broader awareness and a deeper understanding of potential risks. The complexity of securing the cloud demands innovative solutions and continuous vigilance against evolving cybersecurity threats. Active monitoring is key, because future cybersecurity events may involve familiar tools repurposed in innovative, yet unexpected ways.

## Generative AI

Potential for automation and optimization exists, but careful adoption is necessary. Agencies are developing AI policies and identifying use cases for generative AI with a focus on security and data trust. Traditional AI applications differ from the broader, potentially riskier landscape of generative AI.

## Final Thoughts

The future of cloud technology in the federal government is complex. Addressing key concerns around security, vendor lock-in, workforce development and responsible AI integration is crucial to unlocking the cloud's transformative potential.

**Learn more about Palo Alto Network's market leading solutions here: https://www.paloaltonetworks.com/**