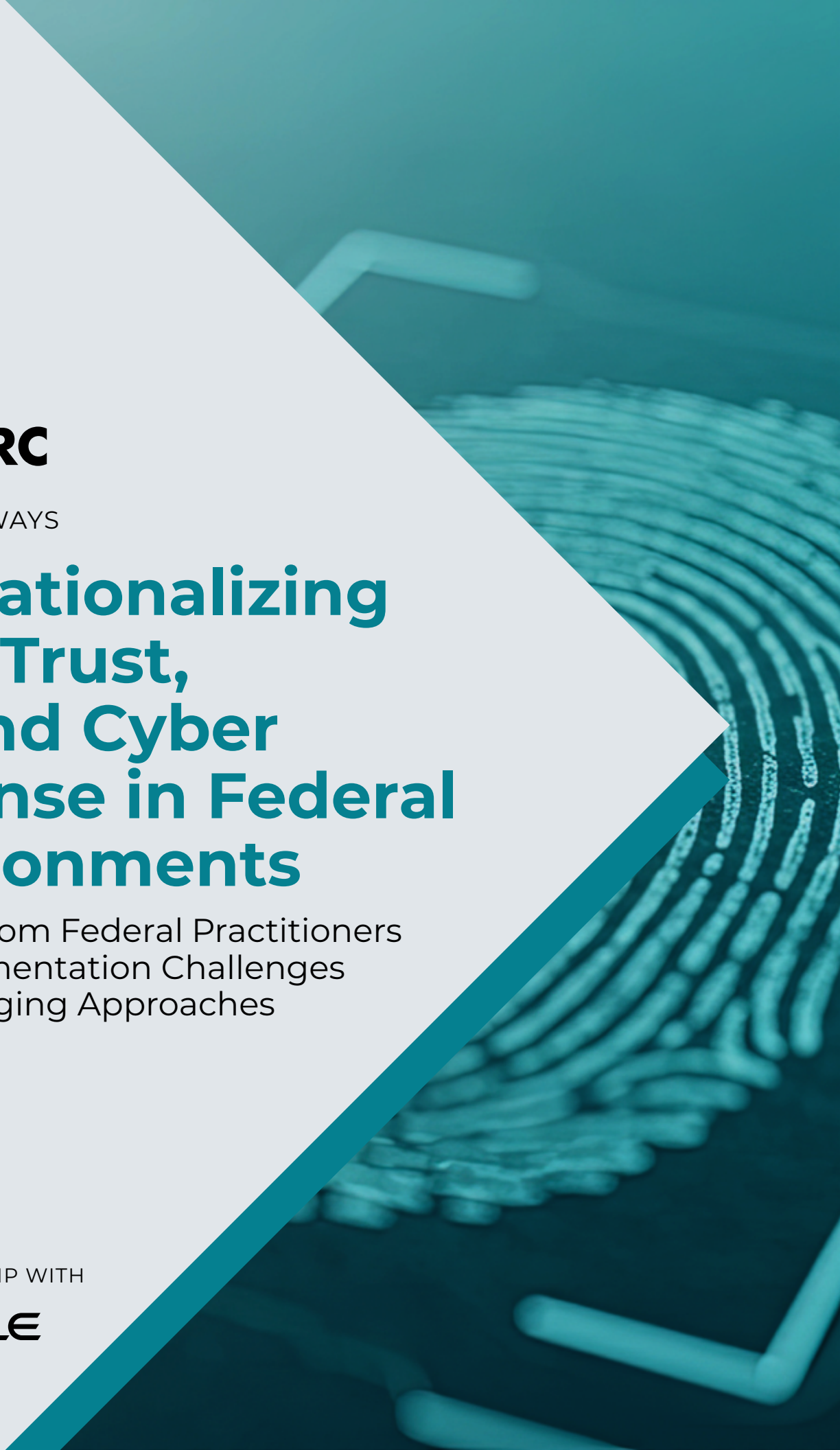
ATARC

TOP TAKEAWAYS

Operationalizing Zero Trust, AI, and Cyber Defense in Federal Environments

Insights from Federal Practitioners on Implementation Challenges and Emerging Approaches



IN PARTNERSHIP WITH

ORACLE

Executive Summary

Federal agencies are under increasing pressure to modernize cybersecurity architectures while maintaining operational agility across diverse mission environments. A recent roundtable of federal practitioners explored the intersection of **Zero Trust architecture (ZTA), artificial intelligence (AI), cloud computing, and cyber defense**, focusing on the practical challenges agencies face when implementing these capabilities.

The discussion, conducted under **Chatham House Rules**, brought together federal cybersecurity leaders, mission operators, technologists, and industry partners to share candid perspectives on operational realities across the federal enterprise. Participants represented organizations responsible for **defense operations, civilian agency systems, oversight functions, and mission-support services**, providing a comprehensive view of the challenges associated with deploying modern cybersecurity architectures across government.

Several key themes emerged from the discussion:

- **Zero Trust remains an architectural integration challenge rather than a single technology deployment.**
- **Legacy systems continue to complicate modernization efforts,** particularly when migrated into cloud environments without redesign.
- **Identity and access management (IAM) remains the foundational challenge** for implementing Zero Trust effectively.
- **Continuous authorization models offer a path to accelerate innovation** while maintaining security.
- **Operational environments—especially disconnected or tactical environments—must be considered in enterprise architectures.**
- **AI is rapidly becoming both a defensive tool and a new attack surface.**

Participants emphasized that federal cybersecurity modernization cannot be achieved solely through policy mandates or compliance frameworks. Instead, agencies must adopt **risk-based implementation strategies**, develop **shared infrastructure and platforms**, and build **operationally resilient architectures capable of supporting mission needs across diverse environments**.

These practitioner insights highlight the importance of aligning **policy, technology, and operational realities** as the federal government advances toward a more resilient and adaptive cybersecurity posture.

Introduction

Cybersecurity modernization has become a central priority across the federal government. In recent years, initiatives such as the **Federal Zero Trust Strategy**, expanded **cloud adoption**, and increased focus on **AI-enabled cyber defense** have driven agencies to rethink traditional security architectures.

However, while federal policies provide direction, the actual implementation of these capabilities remains complex. Agencies operate a wide range of systems, including legacy applications, mission-critical operational platforms, and emerging AI-enabled services. Integrating these systems into a modern security architecture presents significant challenges.

To better understand these issues, federal practitioners gathered for a closed roundtable discussion examining how agencies are navigating the transition to **Zero Trust architectures and AI-enabled cybersecurity capabilities.**

The discussion emphasized practical experience over theory. Participants shared insights from operational environments, highlighting both progress and persistent challenges. As one practitioner noted, modernization efforts often involve **moving legacy systems into cloud environments without fundamentally redesigning them**, effectively transferring existing vulnerabilities into new infrastructure environments.

The conversation underscored a critical reality: implementing modern cybersecurity capabilities across federal systems requires **not only technology upgrades but also organizational, cultural, and operational transformation**.

The Reality of Zero Trust Implementation

Zero Trust architecture has become a cornerstone of federal cybersecurity policy. Yet practitioners emphasized that implementing Zero Trust is significantly more complicated than the conceptual frameworks often suggest.

Participants widely agreed that **there is no single Zero Trust solution**. Instead, agencies must integrate multiple technologies—including identity systems, endpoint security, network segmentation, and monitoring tools—into a cohesive architecture.

Many agencies face the challenge of retrofitting Zero Trust capabilities onto existing infrastructure rather than building systems from scratch. As a result, implementation often requires integrating older systems that were not originally designed with modern security principles in mind.

A practitioner explained that many agencies are still operating in **hybrid environments**, where legacy systems coexist with cloud-based infrastructure and newer digital platforms. This creates complexity when attempting to implement consistent access control and monitoring across environments.

Another participant emphasized that agencies frequently approach Zero Trust as a compliance requirement rather than a strategic architectural shift. This compliance-driven mindset can lead organizations to focus on completing checklists rather than addressing underlying security risks.

Several participants advocated for a **risk-based implementation approach**, where agencies prioritize Zero Trust capabilities based on mission impact rather than attempting to deploy every capability simultaneously.

This approach aligns with guidance encouraging agencies to move away from rigid compliance models toward **risk-informed cybersecurity strategies**.

Identity as the Foundation of Zero Trust

Across the discussion, participants repeatedly emphasized that **identity and access management is the cornerstone of Zero Trust architecture**.

Without robust identity systems, agencies cannot effectively enforce access controls or monitor user activity across distributed environments.

Practitioners noted that identity management challenges often arise when integrating legacy systems that were not designed to support modern authentication models. In many cases, agencies must implement **“identity wrappers”** or intermediary solutions to bridge older systems with modern identity platforms.

Participants also highlighted the importance of implementing **least privilege access controls and dynamic access policies** that adjust permissions based on contextual factors such as user behavior, device status, and location.

However, several participants acknowledged that building comprehensive identity architectures remains difficult. In many cases, agencies rely on multiple identity systems that were developed independently, creating interoperability challenges.

These challenges are compounded by the need to integrate identity systems across multiple agencies, mission partners, and external stakeholders.

As a result, identity management continues to be one of the most complex and resource-intensive aspects of Zero Trust implementation.

Balancing Operational Agility with Security

A central theme of the discussion was the need to balance strong security controls with operational flexibility.

Participants emphasized that overly rigid security processes can slow innovation and delay mission-critical capabilities.

One practitioner highlighted the limitations of traditional **Authorization to Operate (ATO)** processes, which often require lengthy reviews before systems can be deployed.

In response, some organizations are experimenting with **continuous authorization models**, where security assessments are integrated directly into software development pipelines.

These approaches allow agencies to update systems more rapidly while maintaining strong security oversight.

Continuous authorization models are particularly effective in environments where software is deployed using containerized architectures and automated DevSecOps pipelines.

By embedding security checks into development workflows, agencies can identify vulnerabilities earlier and deploy updates more quickly.

Participants suggested that expanding these models across government could significantly accelerate innovation while improving security outcomes.

The Role of Shared Platforms and Infrastructure

Another key discussion point was the importance of shared infrastructure and platform services.

Many federal mission owners lack the resources to build and maintain secure infrastructure independently. As a result, they must rely on enterprise platforms that provide pre-authorized environments for deploying applications.

Participants emphasized that establishing **secure, reusable platforms** can help agencies reduce duplication of effort while accelerating system deployment.

These platforms can provide built-in security controls, monitoring capabilities, and compliance frameworks that individual mission teams can inherit.

By adopting shared platforms, agencies can focus on developing mission-specific applications rather than building security infrastructure from scratch.

However, participants noted that many mission owners still misunderstand how authorization processes work. Some assume that individual applications must obtain their own ATO, rather than deploying within pre-authorized environments.

Addressing these misconceptions will be essential to improving the efficiency of federal system deployment.

Supporting Tactical and Disconnected Environments

While many cybersecurity discussions focus on enterprise networks, participants highlighted the importance of supporting **operational environments with limited connectivity**.

Defense organizations, first responders, and field operations frequently operate in environments where network connectivity is intermittent or unavailable.

These environments require cybersecurity architectures that can function even when disconnected from centralized infrastructure.

Participants discussed emerging technologies designed to address this challenge, including **portable cloud systems**, lightweight computing platforms, and tactical data processing environments.

These solutions allow operational teams to access critical data and applications even when traditional cloud connectivity is unavailable.

One participant noted that these systems must also account for power consumption, physical durability, and security considerations unique to operational environments.

As agencies increasingly rely on cloud computing and AI-enabled tools, ensuring that these capabilities can operate in degraded environments will remain a critical challenge.

Artificial Intelligence in Cyber Defense

Artificial intelligence emerged as a major topic throughout the discussion.

Participants noted that AI is rapidly becoming both a powerful cybersecurity tool and a potential threat vector.

On the defensive side, AI can help agencies analyze large volumes of security data, identify anomalies, and detect emerging threats more quickly than traditional monitoring systems.

However, participants also acknowledged that adversaries are increasingly using AI to develop more sophisticated cyber attacks.

This dynamic creates a **rapidly evolving threat environment**, where defenders must continuously adapt to new techniques.

One practitioner noted that the pace of cyber threats has accelerated significantly, with new attack methods emerging within days rather than months.

This environment requires agencies to adopt **more adaptive security architectures** that can respond to threats quickly.

AI will likely play a central role in this effort, but agencies must ensure that AI systems themselves are properly secured.

Privacy and Data Governance Considerations

Cybersecurity modernization also raises important privacy concerns.

Participants emphasized that agencies must balance the need for data sharing with the requirement to protect sensitive information.

This is particularly challenging in environments where data must be shared across multiple agencies, state and local partners, and international organizations.

Privacy impact assessments and governance frameworks can help agencies evaluate the risks associated with data sharing initiatives.

However, implementing these processes effectively requires close collaboration between cybersecurity teams, privacy officers, and mission stakeholders.

Participants noted that strong privacy protections are essential for maintaining public trust while enabling operational effectiveness.

Cultural and Organizational Challenges

Beyond technical challenges, participants highlighted the importance of addressing cultural and organizational barriers.

Implementing Zero Trust and modern cybersecurity architectures often requires significant changes to existing processes and organizational structures.

In some cases, mission operators may resist security controls that appear to limit operational flexibility.

Conversely, cybersecurity teams may struggle to understand mission requirements.

Participants emphasized the importance of **cross-functional collaboration** between security teams, mission operators, and technology providers.

Developing shared understanding between these groups will be essential to achieving successful modernization outcomes.

The Path Forward

Despite the challenges discussed, participants expressed optimism about the progress federal agencies have made in recent years.

Many organizations have already begun implementing key Zero Trust capabilities, including identity-based access controls, endpoint monitoring, and microsegmentation.

Cloud adoption has also accelerated the deployment of modern infrastructure.

However, participants emphasized that cybersecurity modernization remains an ongoing journey.

Moving forward, agencies will need to focus on several key priorities:

- Expanding identity and access management capabilities
- Developing shared infrastructure platforms
- Implementing continuous authorization models
- Integrating AI into cyber defense strategies
- Ensuring architectures support operational environments
- Strengthening collaboration across agencies and mission partners

Achieving these goals will require sustained investment, strong leadership, and continued collaboration across the federal ecosystem.

Conclusion

The insights shared during this practitioner roundtable highlight the complexity of modernizing federal cybersecurity architectures.

While federal policies provide important direction, real progress depends on the ability of agencies to translate strategic goals into operational capabilities.

Zero Trust architecture, AI-enabled cybersecurity, and modern cloud infrastructure offer powerful tools for improving federal cyber resilience.

However, implementing these capabilities requires addressing technical, organizational, and cultural challenges simultaneously.

By sharing lessons learned and fostering collaboration across agencies, federal practitioners can accelerate progress toward a more secure and resilient digital infrastructure.

The discussion made clear that cybersecurity modernization is not simply a technology initiative—it is an **operational transformation that will shape the future of government mission delivery**.