Multi-Cloud Defense: Redefining the Cyber Playbook
Foreword

The cyber threat landscape is constantly evolving, and the cloud is no exception. Agencies must adapt their cyber strategy through a multi-cloud defense.

The enclosed report, "Multi-Cloud Defense: Redefining the Cyber Playbook" is the product of a partnership between GDIT and MeriTalk to understand the state of cybersecurity in cloud environments across the Federal government. MeriTalk, on behalf of GDIT, surveyed Federal cyber leaders to gain insight into their cybersecurity challenges and opportunities.

The results show agencies understand the fundamental importance of cloud as part of IT modernization and as a driver of innovative cyber capabilities. Unique mission requirements and a complex cloud marketplace challenge agencies to improve their cyber defense. With increased use of AI, machine learning, and a shift towards autonomous cyber and Zero Trust architectures, agencies are placing their focus on the long game.

Of the 90% of survey respondents who already have multi-cloud environments, 84% of them say successful multi-cloud adoption will strengthen their overall cybersecurity posture in the long run. In addition to better cybersecurity, successful multi-cloud adoption will also lead to increased flexibility, cost savings, and mission advancement.

We are pleased to share the enclosed results to help Federal cyber leaders move the ball forward.

Dr. Matthew McFadden
Cyber Director & Distinguished Technologist
Cyber Center of Excellence
GDIT

GDIT Cyber | Secure today. Smarter tomorrow.
Introduction

With 81%* of Federal agencies using more than one cloud platform, multi-cloud environments are government’s new normal.

But how are Feds protecting this rapidly evolving landscape? Are their current cybersecurity tools and strategies adapting fast enough? What steps are they taking to ensure visibility, scalability, resilience, and control?

MeriTalk, on behalf of GDIT, surveyed 150 Federal cyber leaders to explore cybersecurity challenges and opportunities in multi-cloud environments. The Multi-Cloud Defense report catalogs current efforts and aspirations, and offers agency leaders a path to future-proof multi-cloud cybersecurity.

*MeriTalk’s Juggling the Clouds: What Are Agencies Learning?
Agencies are turning to multi-cloud to support telework demands, but cyber strategies aren’t keeping up:

- 83% of Federal cyber leaders say their agency is increasing multi-cloud adoption to support telework and mission needs related to COVID-19.
- 42% are trying to adapt cybersecurity strategies accordingly, but say it’s not fast enough for evolving cloud environments.

Some Feds are taking steps to improve visibility, scalability, resiliency, and control – but more work is needed:

- Only around half of multi-cloud users report taking specific critical steps to secure their environments.
- 52% are deploying cloud-enabled cybersecurity capabilities.
- 46% are increasing data redundancy.
- 46% are automating scaling.
- 36% are automating DevSecOps.

Feds say successful multi-cloud adoption will help future-proof cybersecurity efforts:

- 84% say in the long run, successful multi-cloud adoption will strengthen their overall cybersecurity posture.

To get there, Feds say they need consistency across cloud platforms, automated security policies, and a deeper understanding of their current environments.
Research Findings
Agencies are accelerating multi-cloud adoption to meet telework needs, but 42% say their cybersecurity strategies aren’t keeping pace.

- 83% are increasing multi-cloud adoption to support increased telework and/or mission needs related to COVID-19.
- 76% have begun moving critical services to the cloud to address telework-related availability issues.
- 42% say they are trying to adapt cybersecurity strategies accordingly, but it’s not fast enough to keep pace with evolving multi-cloud environments.

**Takeaway:** As Clouds Multiply, Cyber Strategies Must Catch Up
Feds adopt multi-cloud environments for a variety of reasons, from tech preferences to procurement practices.

Why does your agency have a multi-cloud environment?*

60% To utilize best-of-breed between CSPs
55% Missions procured cloud environments independently
31% Lack of coordination during initial cloud acquisitions

***Takeaway:*** CSP Differentiators and Mission Needs Drive Multi-Cloud Adoption

*Respondents using a multi-cloud environment asked to select all that apply.*
Defense Needs Work

Few multi-cloud users are fully confident in their agency’s cybersecurity posture

**Top challenges to securing multi-cloud:**

- **39%** Budget constraints
- **32%** Difficulty meeting regulatory requirements
- **32%** Lack of skilled workforce
- **31%** Lack of sufficient cybersecurity solutions baked in (such as APIs and ICAM)
- **30%** Increased attack surface

**Takeaway:** Budget, Regulations, and Workforce Hinder Progress

*Accordingly to respondents using a multi-cloud environment; **Respondents using a multi-cloud environment asked to select all that apply*
Focus on the Long Game

91% of all Feds say securing multi-cloud will be a top priority over the next two years

What factors are you prioritizing as you look to secure multi-cloud?*

<table>
<thead>
<tr>
<th>#1</th>
<th>Federal compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>#2</td>
<td>Vulnerability management</td>
</tr>
<tr>
<td>#3</td>
<td>Risk management</td>
</tr>
<tr>
<td>#4</td>
<td>Automated analytics for cyber intelligence</td>
</tr>
<tr>
<td>#5</td>
<td>Network-centric operations</td>
</tr>
</tbody>
</table>

*According to respondents using a multi-cloud environment

Takeaway: Agencies Prioritize Compliance and Vulnerability
Team Efforts

Just half – or fewer – of multi-cloud users report taking critical steps to secure their environments, like utilizing data encryption.

What steps has your agency taken to secure multi-cloud?*

- Utilized data encryption: 51%
- Implemented zero trust principles: 41%
- Adopted FedRAMP-compliant solutions: 39%
- Established centralized controls for threat detection: 38%
- Worked with CSPs to delineate cyber responsibilities: 38%
- Implemented data redundancy: 36%
- Utilized a Cloud Access Security Broker (CASB): 34%
- Deployed cloud-focused cybersecurity stack: 33%
- Adopted automated tools to speed response time (e.g., SOAR): 33%

Takeaway: Making Progress, But More Work Needed

*Respondents using a multi-cloud environment asked to select all that apply.
Breaking Down the Playbook

Visibility | Scalability | Resiliency | Control
First Quarter – Visibility

Just **37%** of multi-cloud users say their current visibility is excellent

Almost all (93%) have taken steps to improve, including:**

- 52% Deploying cloud-enabled cybersecurity capabilities
- 49% Centralizing multi-cloud management teams
- 44% Implementing or expanding access control
- 43% Implementing workload protection platforms
- 40% Adopting cloud management platforms designed specifically for multi-cloud management
- 38% Standardizing data governance policies

**Takeaway:** Despite Steps Taken, Visibility Still Has Its Challenges

*Accordingly to respondents using a multi-cloud environment; **Respondents using a multi-cloud environment asked to select all that apply*
Second Quarter – Scalability

Less than half of multi-cloud users are leveraging automatic scaling

**In what ways is your agency increasing scalability in multi-cloud environments?**

- Scaling automatically (autoscaling) 46%
- Using horizontal scaling (scaling out) 46%
- Scaling at scheduled time 38%
- Using diagonal scaling (up and out) 37%
- Using vertical scaling (scaling up) 32%

**Takeaway: Scale to React in Real Time**

*Respondents using a multi-cloud environment asked to select all that apply*
Third Quarter – Resiliency

Multi-cloud users are taking steps to address resiliency in their environment, but just 37% say their current resiliency is excellent.

Steps taken:

- **46%** Increasing redundancy of data not just in different physical locations, but also with multiple cloud providers
- **43%** Adding services to temporarily house data from one CSP in another during downtime
- **40%** Seamlessly integrating between different providers
- **39%** Enabling CSPs to remotely manage and upgrade services
- **38%** Leveraging a shared cybersecurity capability stack

Takeaway: Build Resiliency with Redundancy, Interoperability

*Respondents using a multi-cloud environment asked to select all that apply.*
Only a third of multi-cloud users have taken key steps like synchronizing policies and implementing SOAR solutions to increase multi-cloud control

**Most common steps?**

<table>
<thead>
<tr>
<th>Step</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronized policies across cloud platforms</td>
<td>36%</td>
</tr>
<tr>
<td>Implemented SOAR solutions</td>
<td>36%</td>
</tr>
<tr>
<td>Adopted continuous monitoring solutions</td>
<td>36%</td>
</tr>
<tr>
<td>Adopted a “single-pane-of-glass” solution</td>
<td>29%</td>
</tr>
<tr>
<td>Automated DevSecOps</td>
<td>36%</td>
</tr>
<tr>
<td>Standardized policy enforcement</td>
<td>35%</td>
</tr>
<tr>
<td>Automated DevOps</td>
<td>35%</td>
</tr>
<tr>
<td>Minimized the number of point cybersecurity solutions</td>
<td>34%</td>
</tr>
</tbody>
</table>

**Takeaway:** Coordinate Automation and Policies for Control

*Respondents using a multi-cloud environment asked to select all that apply; **Security orchestration, automation, and response
Going for the Win

Overall, Feds say multi-cloud adoption will improve cybersecurity across government

How will agencies measure success?*

45% Improved CapEx compared to previous environments
44% Improved ability to meet the mission owner’s requirements
42% Optimized user experience
42% Improved metrics from tools monitoring the before and after
42% Improved OpEx compared to previous environments

Takeaway: Promote Cost Reductions and Mission Advancements

*Respondents using a multi-cloud environment asked to select all that apply

84% say successful multi-cloud adoption will strengthen their agency’s overall cybersecurity posture in the long run
Road to Victory

Feds see successful multi-cloud adoption benefiting Federal agencies in the COVID-19 era and beyond

What are the long term benefits of multi-cloud adoption?*

- Security: 53%
- Flexibility/scalability: 51%
- Cost savings: 49%

*All respondents asked to select all that apply

Takeaway: Multi-Cloud is a Game-Changer
Looking ahead, Feds want greater consistency, automation, and understanding

“Consistency across cloud platforms is key to moving multi-cloud forward … and future-proofing infrastructure and operations across public, private, and edge environments”

“We need to automate our security policies across multiple networks”

“Evaluate the effectiveness of existing solutions and determine whether cloud instances are configured correctly”

“Understand the cloud environment better, know the endpoints and the pass-throughs, and understand where the weaknesses are in security and infrastructure”

“Minimize downtime and maximize reliability and redundancy”
Focus on agility
As clouds continue to multiply, Federal cyber strategies must evolve to keep up. IT teams and agency leadership must meet regularly to review the state of play, confirm priorities, and adjust to ever-evolving threats.

Centralize management
Many agencies found themselves in multi-cloud environments due to disparate cloud adoption. Going forward, Feds should work toward consistency across platforms to streamline management and apply holistic cybersecurity.

Elect automation team captain
Federal cyber leaders are actively working to improve multi-cloud visibility, scalability, resiliency, and control. Agencies should look to automation in areas like scaling, analytics, policy, and DevSecOps to move the ball forward.
Methodology & Demographics

MeriTalk, on behalf of GDIT, conducted an online survey of 150 Federal cyber leaders familiar with their agency’s cybersecurity efforts in cloud environments in May and June 2020. Of the Federal cyber leaders, 90% say they are multi-cloud users. The report has a margin of error of ±7.97% at a 95% confidence level.

Respondent job titles

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-suite (CIO, CTO, CISO, or other executive-level IT decision-maker)</td>
<td>22%</td>
</tr>
<tr>
<td>IT Director, Manager, or Supervisor</td>
<td>51%</td>
</tr>
<tr>
<td>Cybersecurity Program Manager/Officer</td>
<td>10%</td>
</tr>
<tr>
<td>Cybersecurity Analyst/Engineer/Specialist</td>
<td>7%</td>
</tr>
<tr>
<td>Cybersecurity Acquisitions/Procurement Manager</td>
<td>2%</td>
</tr>
<tr>
<td>Software/Applications Development Manager</td>
<td>6%</td>
</tr>
<tr>
<td>Data Center or Network Manager</td>
<td>1%</td>
</tr>
<tr>
<td>Cloud Specialist/Engineer</td>
<td>1%</td>
</tr>
</tbody>
</table>

Organization types

<table>
<thead>
<tr>
<th>Organization Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Government: Civilian agency</td>
<td>41%</td>
</tr>
<tr>
<td>Federal Government: DoD agency</td>
<td>36%</td>
</tr>
<tr>
<td>Federal Government: Intelligence agency</td>
<td>23%</td>
</tr>
</tbody>
</table>

Expertise

100% of qualifying respondents were familiar with their agency’s cybersecurity efforts in cloud environments.