Multi-Cloud Defense: Redefining the Cyber Playbook

GDIT | Art of the Possible

Presented by

GENERAL DYNAMICS
Information Technology

In Partnership with

MeriTalk
Improving the Outcomes of Government IT

Contents

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

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.

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

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?

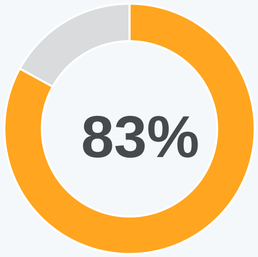
MeriTalk, on behalf of GDIT, surveyed 150 Federal cyber leaders to explore cybersecurity challenges and opportunities in multi-cloud environments. The **Multi-Cloud Defense** report catalogs current efforts and aspirations, and offers agency leaders a path to future-proof multi-cloud cybersecurity.

*MeriTalk's Juggling the Clouds: What Are Agencies Learning?

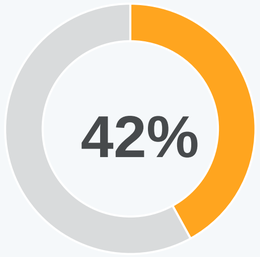
© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Executive Summary

Agencies are turning to multi-cloud to support telework demands, but cyber strategies aren't keeping up:



of Federal cyber leaders say their agency is increasing multi-cloud adoption to support telework and mission needs related to COVID-19



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 capbabilities

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

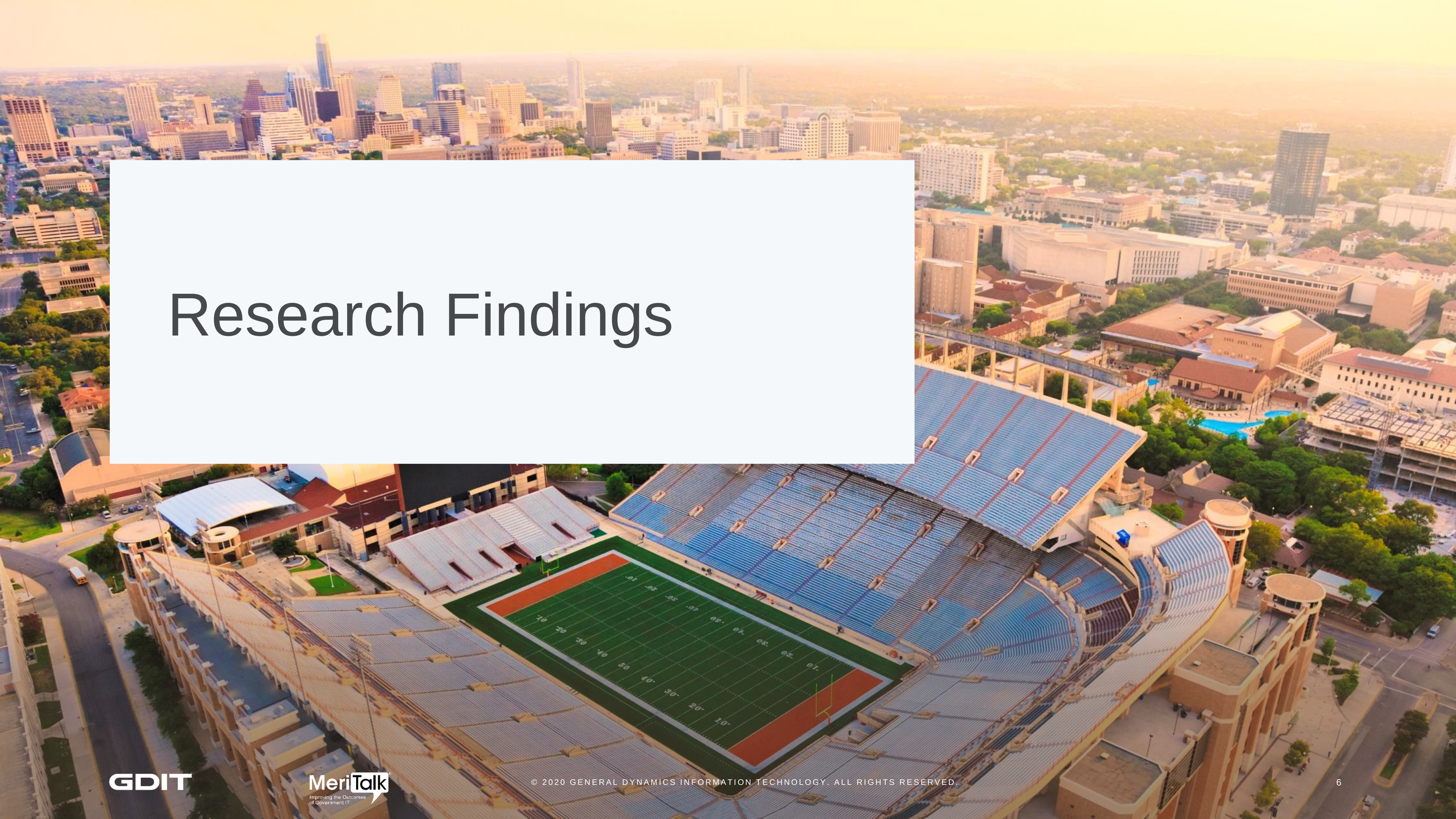
To get there, Feds say they **need** consistency across cloud platforms, automated security policies, and a deeper understanding of their current environments

GDIT

MeriTalk
Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

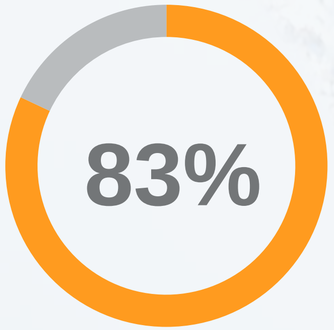
Research Findings



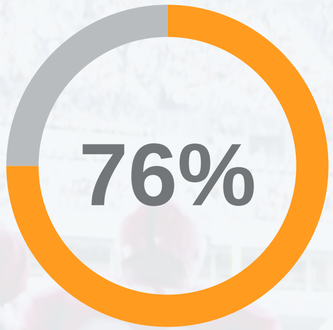
© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Game Time

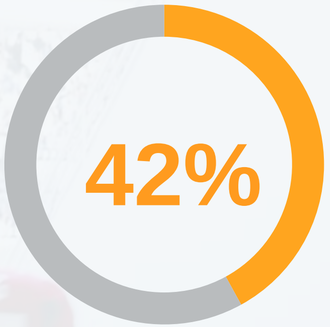
Agencies are accelerating multi-cloud adoption to meet telework needs, but 42% say their cybersecurity strategies aren't keeping pace



are **increasing multi-cloud** adoption to support increased telework and/or mission needs related to COVID-19



have begun moving **critical services** to the cloud to address telework-related availability issues



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

GDIT MeriTalk Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Player Motivations

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

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

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

Only a **quarter** give their agency an '**A**' for their overall multi-cloud cybersecurity posture*

GDIT

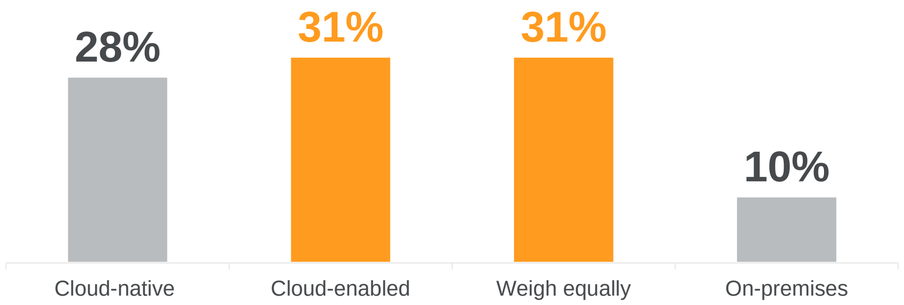
MeriTalk Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Focus on the Long Game

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

How does your agency prioritize cloud-native vs. cloud-enabled cybersecurity solutions?



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

#1	Federal compliance
#2	Vulnerability management
#3	Risk management
#4	Automated analytics for cyber intelligence
#5	Network-centric operations

*According to respondents using a multi-cloud environment

Takeaway: Agencies Prioritize Compliance and Vulnerability

GDIT

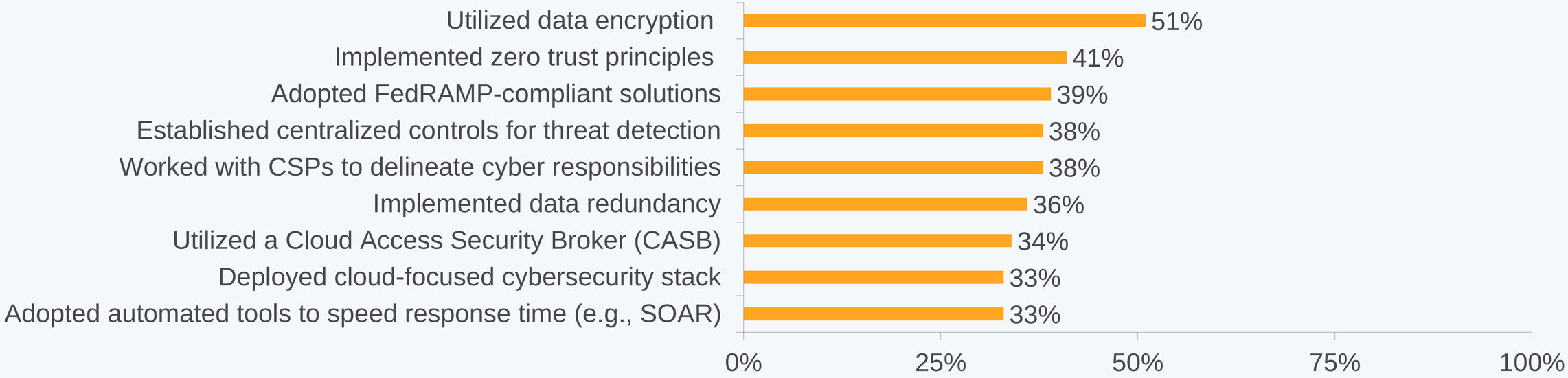
MeriTalk
Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Team Efforts

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

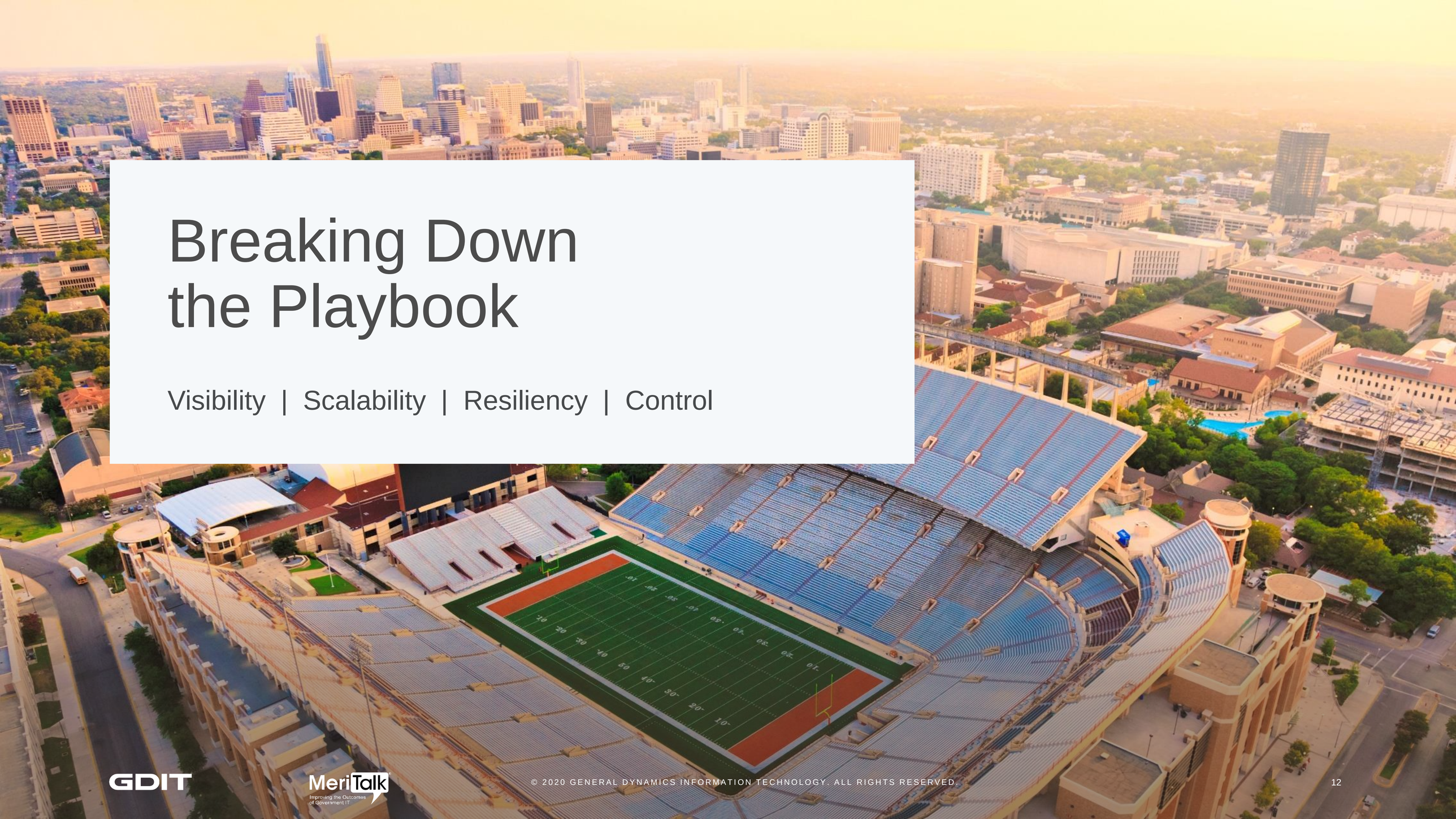
What steps has your agency taken to secure multi-cloud?*



Takeaway: Making Progress, But More Work Needed

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

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.



Breaking Down the Playbook

Visibility | Scalability | Resiliency | Control

GDIT

MeriTalk
Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

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

GDIT

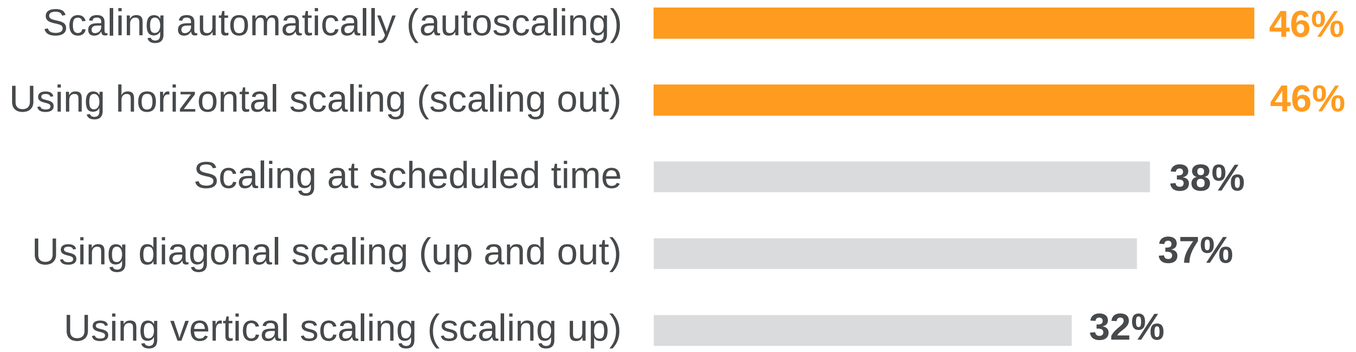
MeriTalk Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

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?*



Takeaway: Scale to React in Real Time

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

GDIT

MeriTalk
Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

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 down time

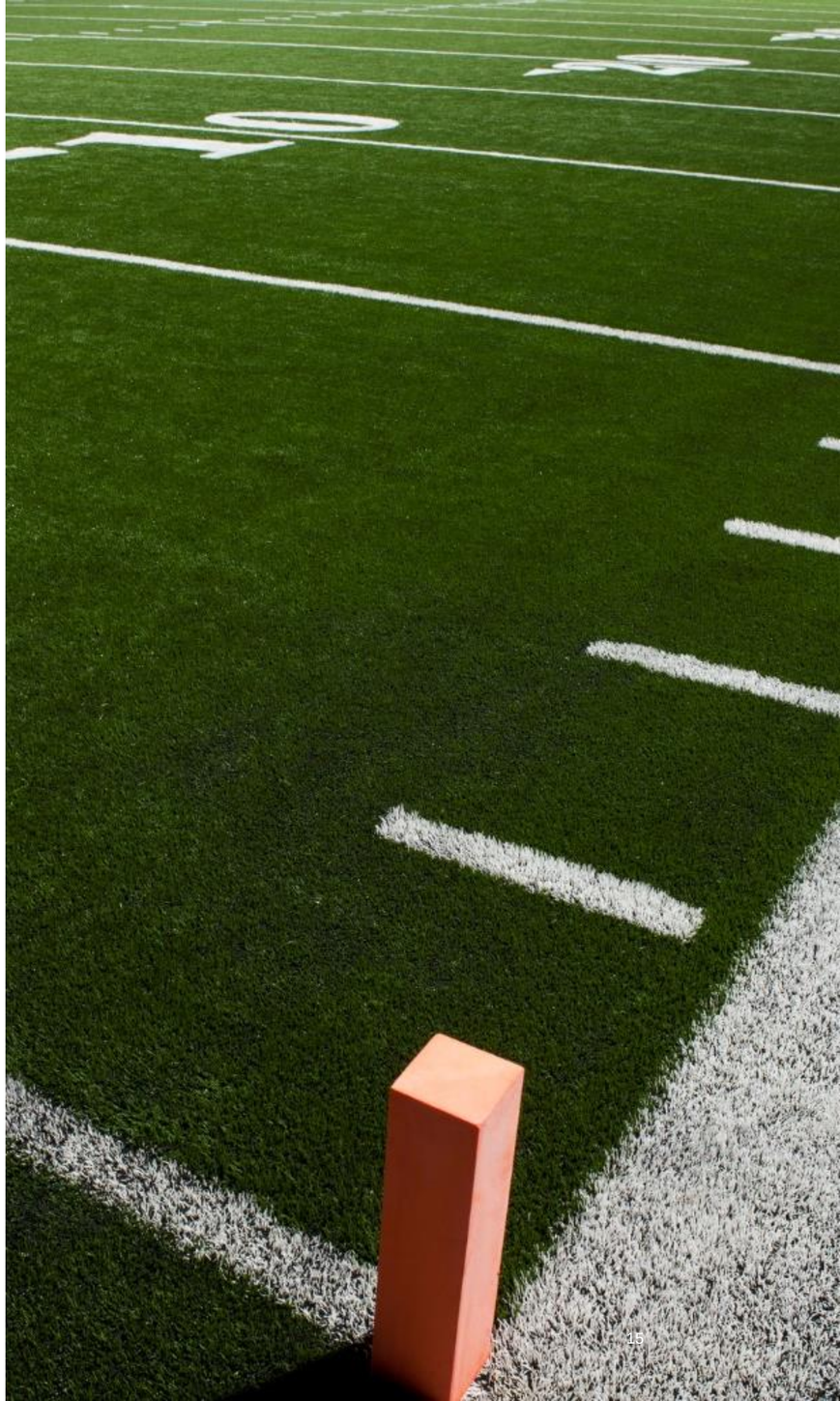
40% Seamlessly integrating between different providers

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

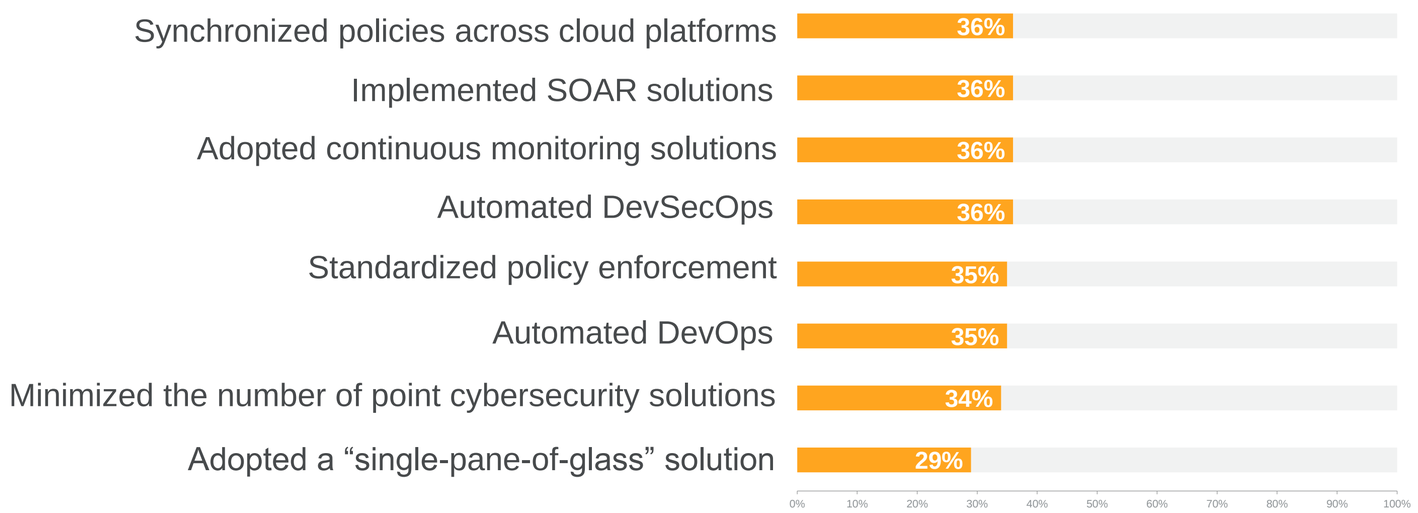


© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Fourth Quarter – Control

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?*



Takeaway: Coordinate Automation and Policies for Control

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

GDIT

MeriTalk Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

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

GDIT

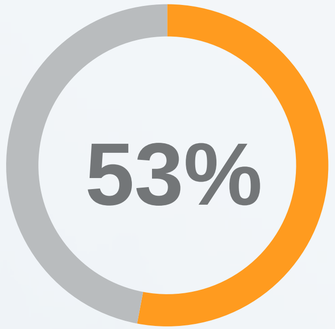
MeriTalk Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Road to Victory

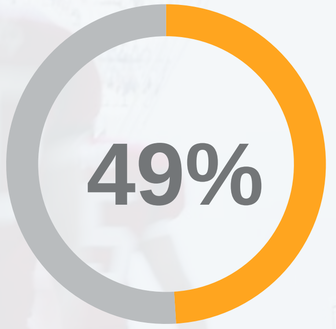
Feds see successful multi-cloud adoption benefiting Federal agencies in the COVID-19 era and beyond

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



Security

Flexibility/scalability



Cost savings

Takeaway: Multi-Cloud is a Game-Changer

*All respondents asked to select all that apply

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Coaching for the Future

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”

GDIT

MeriTalk Improving the Outcomes of Government IT

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

Recommendations

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.

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

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

C-suite (CIO, CTO, CISO, or other executive-level IT decision-maker)	**22%**
IT Director, Manager, or Supervisor	**51%**
Cybersecurity Program Manager/Officer	**10%**
Cybersecurity Analyst/Engineer/Specialist	**7%**
Cybersecurity Acquisitions/Procurement Manager	**2%**
Software/Applications Development Manager	**6%**
Data Center or Network Manager	**1%**
Cloud Specialist/Engineer	**1%**

Organization types

Federal Government: Civilian agency	**41%**
Federal Government: DoD agency	**36%**
Federal Government: Intelligence agency	**23%**

Expertise

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

© 2020 GENERAL DYNAMICS INFORMATION TECHNOLOGY. ALL RIGHTS RESERVED.

GENERAL DYNAMICS
Information Technology

MeriTalk
Improving the Outcomes of Government IT