To Cloud or Not to Cloud? That Isn’t the Question...

October 24, 2017

Underwritten by: FORTINET

Introduction

MeriTalk
Improving the Outcomes of Government IT

With the non-stop cloud chatter, too many Federal agencies think they need to choose between "all cloud" and "no cloud at all." But the reality is not either, **it's both**. While cloud adoption may be stealing the show, agencies still plan to maintain on-premises data centers. For most, the end result will be a combination of physical servers, private, and public cloud – a hybrid (and sometimes multi-cloud) environment.

Instead of "**To Cloud or Not to Cloud?**" the question becomes how can Feds manage and secure this complicated new mix of physical and virtual appliances? How can they protect their enterprise infrastructure and all-important data among complex collaborations with other departments, agencies, and external cloud providers? What's working, and what do agencies still need?

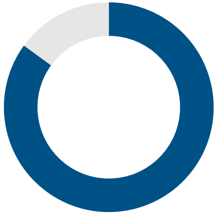
To find out, MeriTalk surveyed **150 Federal IT managers** familiar with their agency's security efforts both inside and outside of cloud. Cue the results…

Executive Summary

- Hybrid Cloud Takes Center Stage:
  - Federal IT managers want to move more of their infrastructure from physical servers to cloud – but not all of it. Feds say their ideal mix includes **39%** physical servers and **61%** cloud
  - **70%** believe that in 10 years, the majority of Federal agencies will rely on hybrid cloud environments for core applications
- Security Woes Bring Down the House:
  - Federal IT managers say their **#1** cloud challenge is expanding security measures and policies to cover cloud environments, and **more than half** say their current level of complexity and lack of visibility is putting them at significant risk for a security breach
  - While nearly half say hybrid cloud environments have made complexity, visibility, and security easier to manage, roughly ***the same or more*** say it's made things more difficult
- With Proper Prep, Feds See Smashing Potential:
  - Agencies with "**excellent**" security integration between physical and cloud environments are significantly more likely than others to apply a third-party security fabric, integrate security into a SIEM, and centralize management
  - In the long run, Feds believe successful hybrid cloud adoption will reduce their agency's security spending (**70%**) and strengthen their overall security posture (**69%**)

Setting the Scene

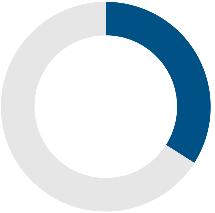
- Federal agencies face significant security threats due to overly complex infrastructure environments and a lack of visibility



85%

of Federal IT managers say their current infrastructure environment is complex*

and just



34%

have a high level of visibility into that same environment**

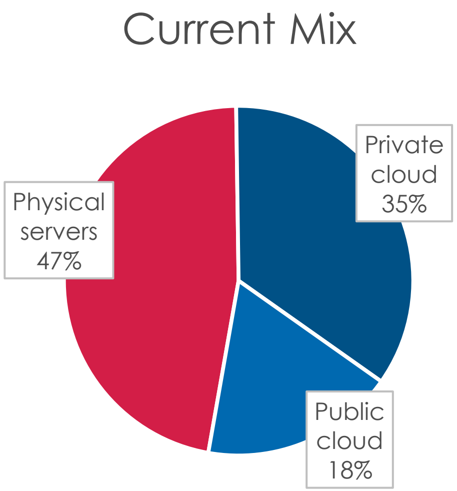
Federal IT managers say the current complexity (54%) and lack of visibility (53%) into their agency's infrastructure environment puts them at significant risk for a security breach

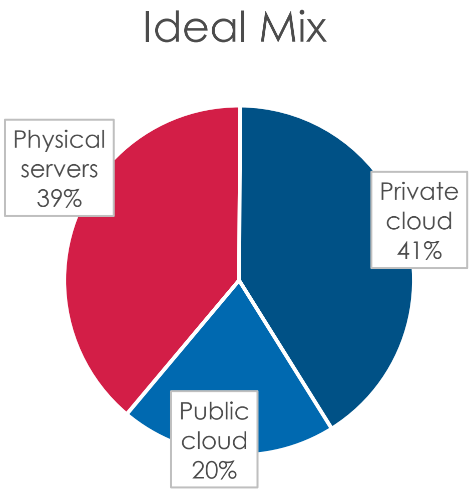
Take away: Not Ready for Opening Night

*Percentage who rated their agency's infrastructure complexity a 6-10 on a scale of 1-10, where 1 is not at all complex and 10 is extremely complex
**Percentage who rated their agency's infrastructure visibility a 8-10 on a scale of 1-10, where 1 is no visibility and 10 is perfect visibility

Mounting Tension

- Federal IT managers want to move more of their infrastructure from physical servers to cloud – but not all of it. Feds say their ideal mix includes **39%** physical servers and **61%** cloud





70% believe that in 10 years, the majority of Federal agencies will rely on **hybrid cloud** environments for core applications

Take away: Hybrid Takes Center Stage

Stage Fright

- Feds say expanding security measures and policies to cover cloud environments is the #1 challenge of the cloud journey

How would you rate your agency's current security management in each of the following environments? Percentage who say "excellent":

35%
in private clouds

21%
in public clouds

27%
while moving between physical and virtual environments

Take away: Security Woes Bring Down the House

Production Challenges

- Feds say data protection issues and compliance challenges hold them back from successful hybrid adoption

Top security concerns when managing a hybrid cloud environment:*

#1
Data protection

#2
Compliance with Federal mandates

#3
Encryption of stored data

#4
Endpoint security

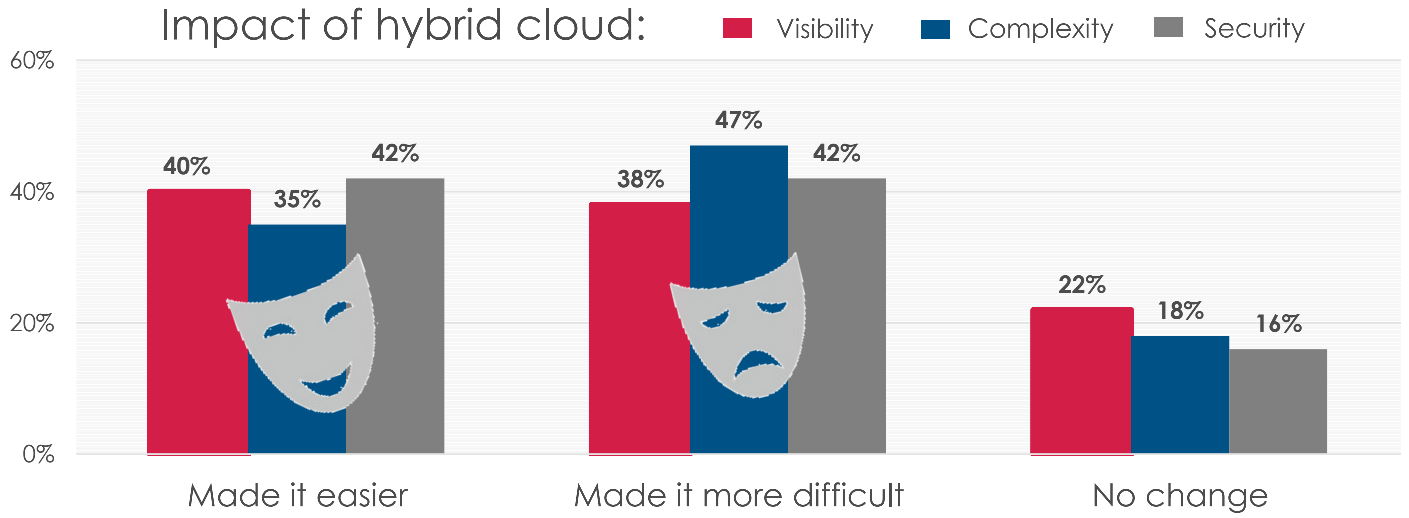
#5
Data misuse

Take away: Data Receives Top Billing

*Respondents asked to select all that apply

Comedy or Tragedy?

- Overall, agencies are split on hybrid's impact on visibility, complexity, and security – half say it helps, half say it hurts



Take away: Perplexing First Act

Managing a Full House

- The good news: **87%** of Feds use formal governance policies to help protect their infrastructure while working with other departments, agencies, and external cloud providers

Top governance strategies:*

49%	Known systems of record
44%	Defined/identified data owners
39%	Quality, documented metadata
38%	Well-understood data integration processes

Initial impact:

Those employing two or more of these governance strategies are significantly more likely to say hybrid adoption has had a positive impact on their infrastructure complexity – 43% to 26%

Take away: Clear Direction Eases Complexity

*Respondents asked to select all that apply

Working Out the Kinks

- While just **27%** of Feds rate the level of security integration between their agency's physical and virtual environments as excellent*, those who do take specific steps to succeed

Agencies that rate their security integration as **excellent*** are significantly more likely than those who do not to:

1. Apply a third-party security fabric or other virtual network security services to enable consistent security enforcement across a distributed network environment – 46% to 15%

2. Integrate security into a SIEM or other analytic tool with the ability to gather and correlate data – 46% to 17%

3. Centralize management for automatic provisioning of multi-layered workload security – 46% to 33%

Take away: Integration is the Star

*In terms of automated security alerts and corrections

The Show Must Go On

- Feds say improved visibility, data segmentation, and centralized management will further support security efforts

How do you think your agency could better leverage integration and automation to ensure swift security intelligence?

"Improve **visibility** and actionable alerts"

"Use more **AI** to identify and isolate potential threats immediately"

"Apply higher levels of data management and **segmentation** for more secure and available data"

"Use more **centralized control** and actual execution of policies versus centralized control and decentralized application of those policies"

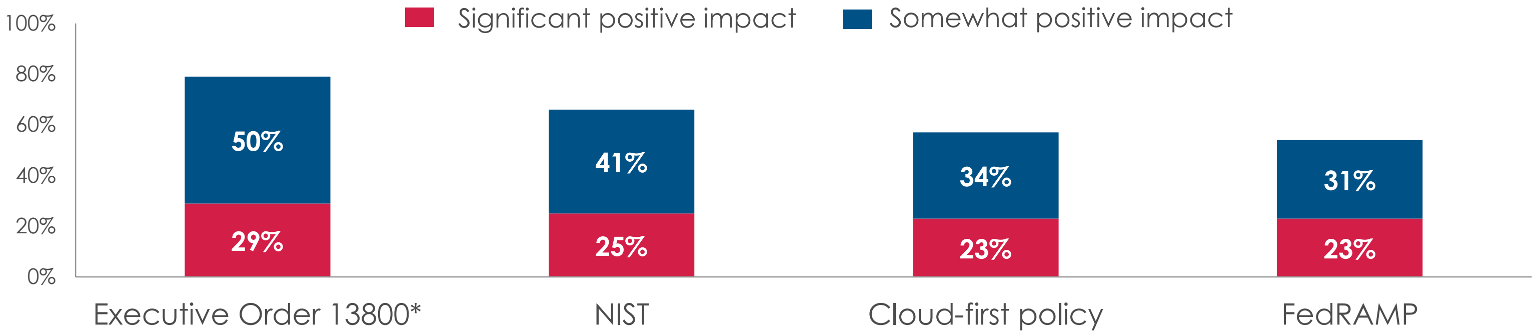
"Leverage threat intelligence sharing, **integrate intelligence feeds**, use automated remediation, etc."

Take away: Set Up for Success

Supporting Cast

- Federal mandates help usher in hybrid cloud environments

Percentage of Feds who say the following have had a positive impact on their ability to successfully utilize a hybrid environment



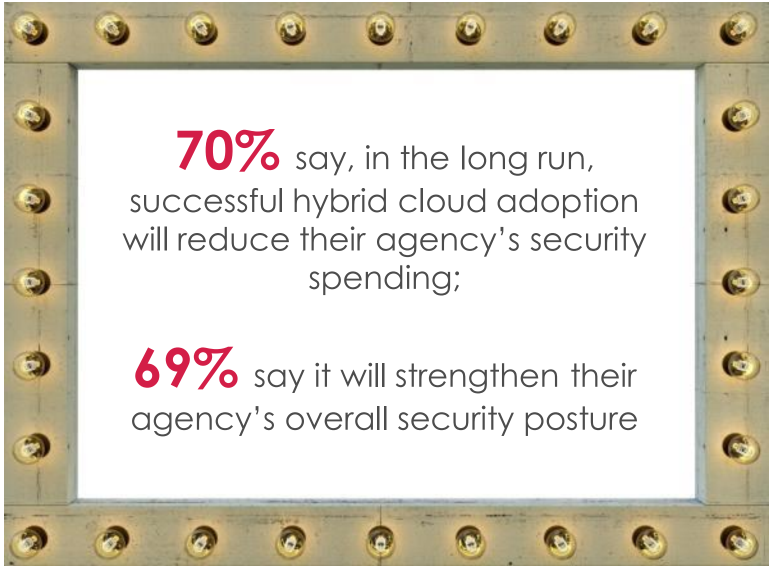
Federal civilian agencies are more than twice as likely as DoD agencies to say FedRAMP and the Cloud-first policy have had significant positive impacts – 27% to 12% in both cases

Take away: Latest EO Gives the Biggest Lift

*Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Potential Smash

- Feds say hybrid environments are poised to strengthen security and increase overall efficiency



70% say, in the long run, successful hybrid cloud adoption will reduce their agency's security spending;

69% say it will strengthen their agency's overall security posture

Top benefits of a hybrid cloud environment:*

47%	Improved efficiency
46%	Reduced overall costs
39%	Improved performance
33%	Improved scalability
30%	Reduced capital expenditures
30%	Enable staff to focus on more critical tasks
27%	Improved continuity of operations
25%	Improved innovation

Take away: Cloud Crowd Pleaser

*Respondents asked to select all that apply

Lessons from Past Performances

- Feds see consistent connectivity, governance, and expert support as critical factors for successfully managing and securing hybrid cloud environments

What is the most significant lesson your agency has learned so far about managing and securing a hybrid cloud environment?

- "Access to these cloud applications rely heavily on our network infrastructure and the ability to reach those applications"
- "Local agency expertise is very sparse and we have to rely more on service providers for implementation"
- "Having a clear vision and buy-in from stake holders is essential for any significant changes"
- "Make sure all procedural complexities are explored and secured in the process"
- "The cloud environment is constantly evolving. Once you think you have it figured out, there is a new app, security patch, or hardware to take it to the next level"

Take away: Study the Show Notes

Recommendations

Update a Classic

Feds see hybrid cloud environments as core to future applications. But agencies must address infrastructure complexities and visibility issues before they can experience the full benefits of a successful hybrid environment

Take to New Talent

While agencies see securing cloud as a daunting task, automation can ease the workload. By centralizing management and considering third-party tools, Feds can improve efficiencies and outcomes

Utilize Supporting Cast

Strong governance policies and recent Federal mandates are helping move hybrid in the right direction. Agencies should lean on both to maintain authority over physical and virtual appliances, and ensure top-down support

EVERY CLOUD ENGENDERS NOT A STORM

WILLIAM SHAKESPEARE

Methodology & Demographics

MeriTalk
Improving the Outcomes of Government IT

MeriTalk, on behalf of Fortinet, conducted an online survey of 150 Federal IT managers familiar with their agency's security efforts, both inside and outside of cloud, in September 2017. The report has a margin of error of ±7.97% at a 95% confidence level.

Respondent Job Titles

CIO/CTO/CISO	9%
Deputy CIO/CTO/CISO	5%
IT Director/Supervisor	24%
Security Analyst/Engineer	15%
Security Architect/Administrator/Specialist	9%
Software/Applications Development Manager	7%
Network Administrator	5%
Data Center Administrator	3%
Enterprise or Mission IT Operations Manager	9%
IT Development Manager	7%
Other IT Manager	7%

Agency Type

Federal Government: Civilian agency	49%
Federal Government: Department of Defense (DoD)	40%
Federal Government: Intelligence agency	11%

Expertise

100% of qualifying Federal IT managers are familiar with their agency's security efforts, both inside and outside of cloud

Thank You

www.meritalk.com 🌐

smasuda@meritalk.com ✉

703-883-9000 ext. 126 📱