MeriTalk
Improving the Outcomes of Government IT

Federal Cybersecurity in a Changing World

June 22, 2020

Underwritten by:

Forcepoint

Introduction

Federal cybersecurity is more critical than ever as agencies quickly adapt to a "maximized telework" environment. But, how effective are Feds' current cybersecurity efforts?

What is working well in agencies' cybersecurity strategies, and what needs to change? If agencies could rebuild their strategies from the ground up, what would they look like?

MeriTalk surveyed **150 Federal IT managers** and compiled qualitative data from in-depth **interviews with Federal cybersecurity leaders** to understand the state of cybersecurity in Federal agencies and offer recommendations to advance cyber progress.

Executive Summary

- Cybersecurity is a top priority, but attention is not converting to action:
  - **84%** of Federal IT managers agree cybersecurity is a top or high priority within their agency
  - Yet, just **51%** rate the state of cybersecurity within their agency as "very effective" and only **34%** say their senior leadership is fully engaged

- Leading agencies focus on cyber agility and communication:
  - **78%** of self-described cyber 'leaders' review, update, and implement their cybersecurity strategy on an ongoing basis
  - Leaders are also significantly more likely than non-leaders to prioritize increasing **agility** vs. reducing costs, and say their agency's secretary has an excellent understanding of their cybersecurity ROI

- Moving forward, Feds see the ideal cyber strategy as proactive and risk-focused:
  - If given the chance to rebuild their strategy, Feds would start with **a zero-trust** model and ensure **full-scope visibility** into the network
  - To get there, Feds say they'll need to overcome budget and legacy challenges, defend against malware, and derive value from innovative security technologies like **artificial intelligence**

Current Cyber Snapshot

We're used to the old castle and moat approach.
But now that we're getting more dispersed,
how are we managing the risks?

Current State of Federal Cybersecurity

- Despite an increased focus on cybersecurity due to widespread telework demands, just half of Federal agencies feel their efforts are "very effective"

77% say their agency's focus on cybersecurity has **increased** over the last month or so due to changing telework demands

While **87%** say their security team is consistently **ahead of cybersecurity threats**,

JUST

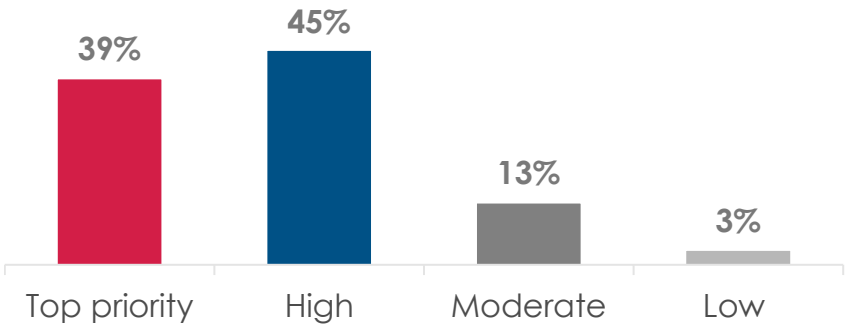
51% describe the state of cybersecurity in their agency as "**very effective**"

Takeaway: A Step Ahead May Not Be Enough

Cyber Significance

- Cybersecurity is a high priority for Federal agencies, but just **34%** say their senior leaders are fully engaged with it as part of their organizational strategy

When your agency assesses the risk factors facing it, what level of priority is assigned to cybersecurity?



34% say their agency's senior leadership recognizes that **cybersecurity is critical**, and is **fully engaged** with it as part of a key organizational strategy

Takeaway: Increase Value with Top-Down Engagement

Evolving Threats

- Two-thirds (**66%**) of Federal IT managers say the possibility of being the next headline-grabbing cybersecurity breach keeps them up at night

Biggest challenges to formulating your agency's cybersecurity strategy?*

#1 Understanding evolving cybersecurity threats (42%)

#2 The challenges of migrating to the cloud (37%)

#3 Understanding technical vulnerabilities (34%)

#3 Lack of collaboration between agency leaders and security leaders (33%)

#5 Identifying vulnerable assets (30%)

Takeaway: Continual Education & Adaptive Strategies Needed

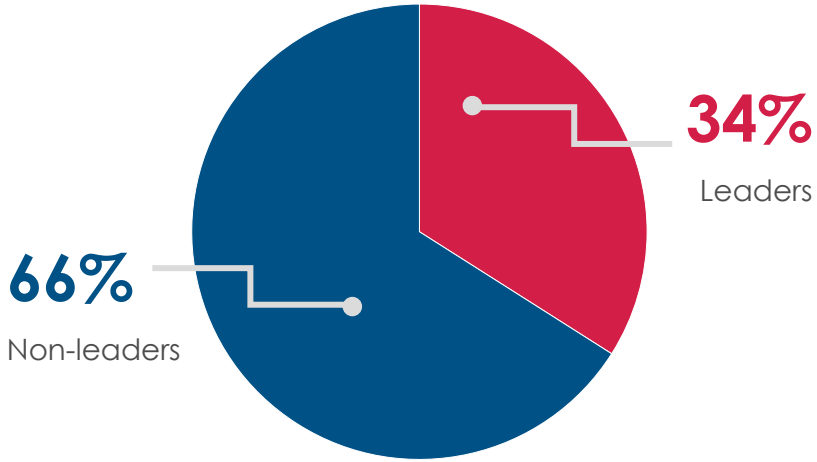
*Respondents asked to select the top three

Federal Cyber Leaders

We have a really good cyber program based on three pillars – people, process, and technology… Without one of those three pillars, the house falls

The Leaders Emerge

- When asked to rate their agency's cybersecurity effectiveness relative to their government peers, **34%** of Feds described themselves as 'Leaders'



Leaders are significantly more likely to give their agency the highest possible rating in:

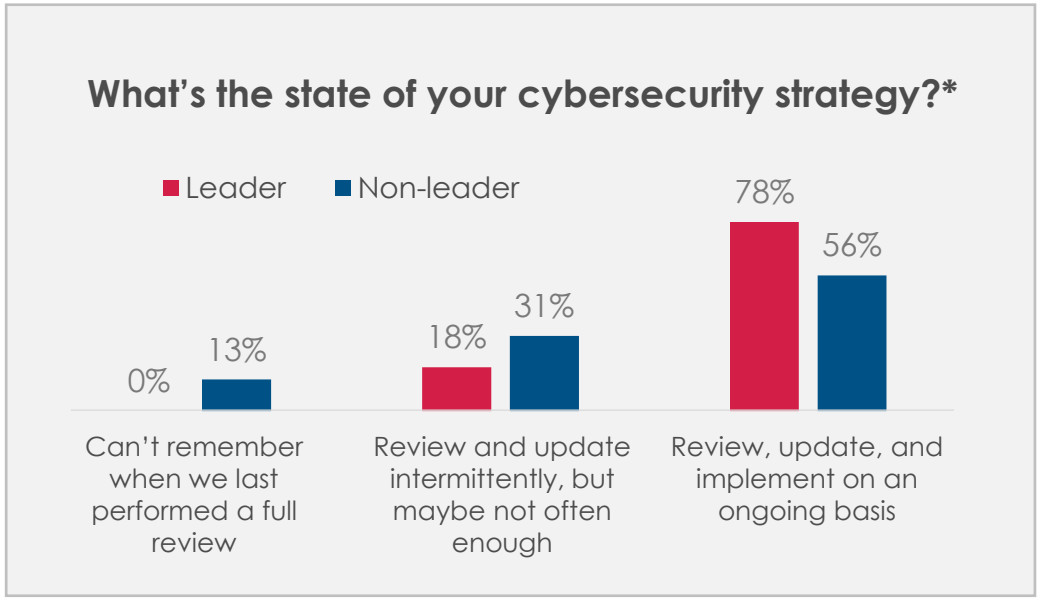
- Digital maturity (**63%** to **23%**)
- Cybersecurity talent (**75%** to **25%**)

They're also more likely to strongly agree that their cyber strategy is a **major driver** of organizational and digital transformation – **57%** to **38%**

Takeaway: What Can We Learn?

Strategy Review

- **78%** of Leaders review, update, and implement their cybersecurity strategy continually



Leaders are also **more likely** than non-leaders to say their senior executives and the CISO **check in at least weekly**

"There's a lot of willingness from all partners and players involved to be successful" – Federal cyber leader

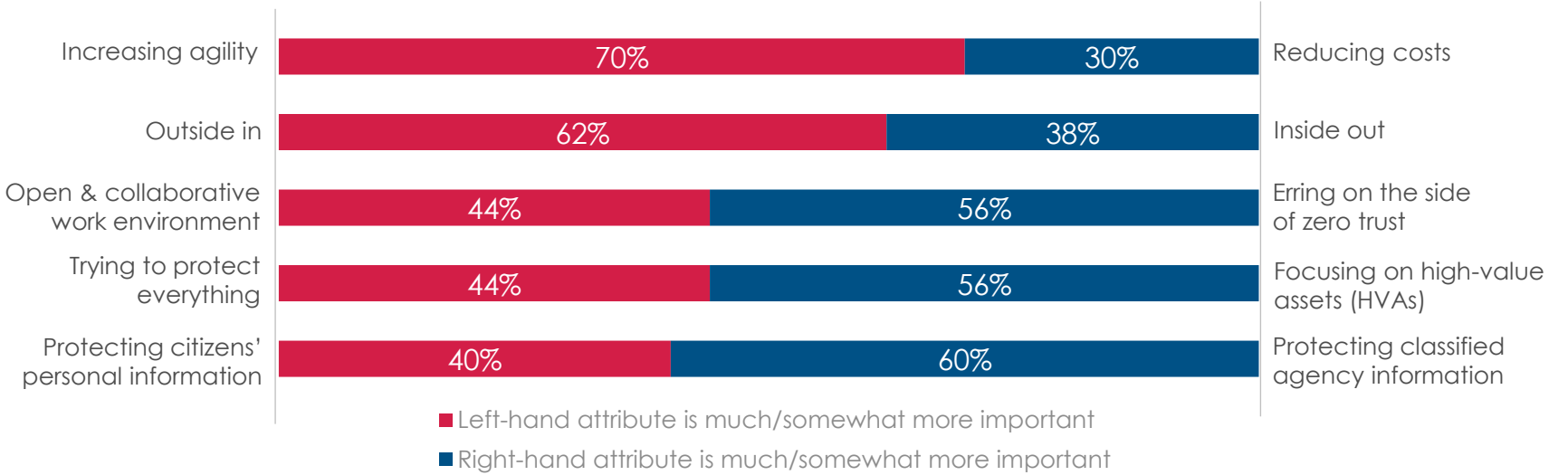
Takeaway: Persistent Updates are a Must

*The remaining respondents do not have a formal policy

Current Priorities

- Federal cyber strategies are focused on increasing agility, preventing intruders, and protecting classified information. Leaders are even more likely to prioritize agility than non-leaders – **84%** to **63%**

All: Where is your strategy positioned across the following dimensions?*



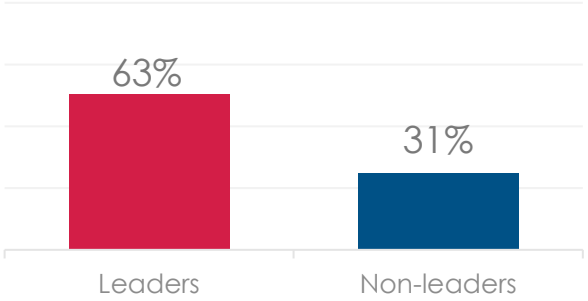
Takeaway: Agility Leads; Zero Trust and HVAs Have Slight Edge

*Does not include percentage who said these are equally important

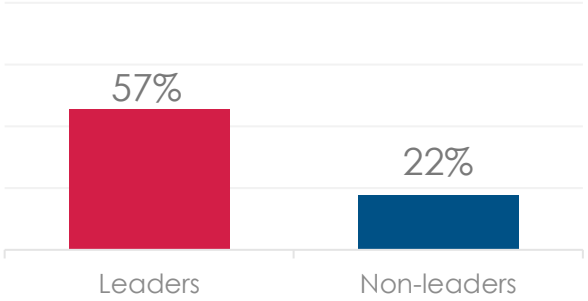
Rating the Return

- Leaders are significantly more likely to rate their cybersecurity ROI as excellent and say their agency's secretary has an excellent understanding of cybersecurity ROI

Rate the **return** on their agency's cybersecurity investments as excellent:



Rate their agency secretary's **understanding** of cybersecurity ROI as excellent:



"Partner with the business side to fully enable them to do what they need to do" – Federal cyber leader

Takeaway: Leaders Communicate Cyber ROI

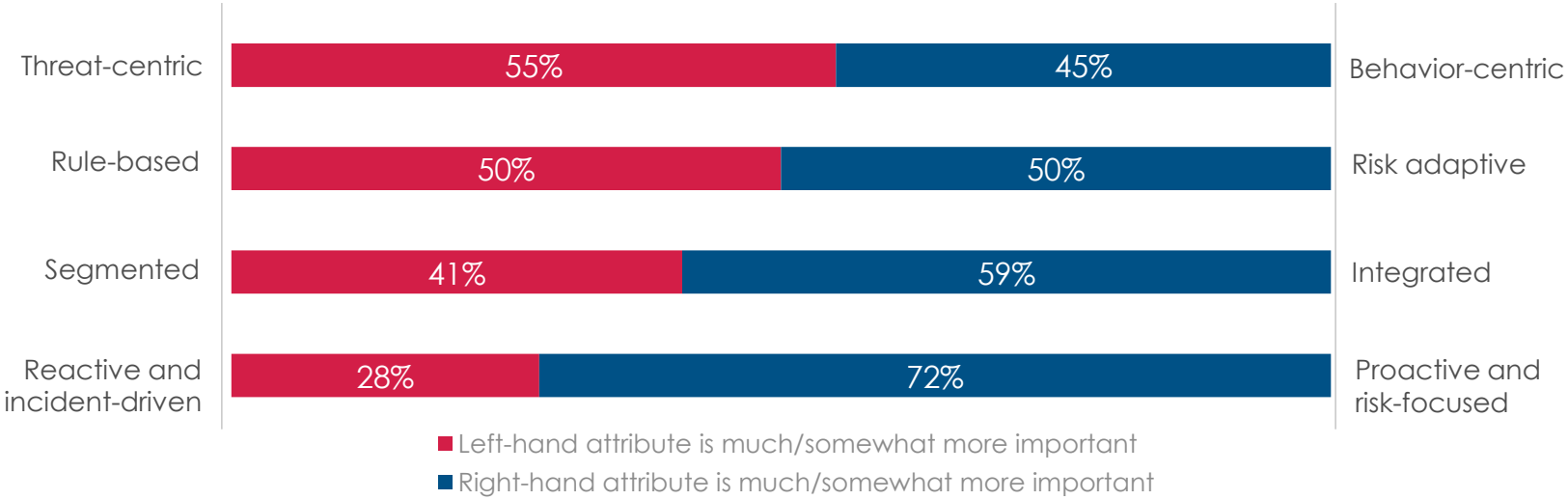
Reimagining Federal Cybersecurity

We need a whole new paradigm shift around how we think about [cybersecurity]… We need to ensure senior leaders in Congress understand the power and impact cyber can have

Ideal System

- Feds agree the ideal cybersecurity strategy is proactive and risk-focused. Leaders are significantly more likely than non-leaders to prefer a rule-based approach – **63%** to **44%**

All: Where would the ideal cybersecurity strategy be positioned?*



Takeaway: Proactivity Tops Cyber Goals

*Does not include percentage who said these are equally important

Cyber Roadblocks

- However, only **11%** of Feds say their agency's current cybersecurity is **identical** to the ideal system they described

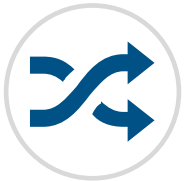
Obstacles preventing agencies from implementing the ideal system:*

Budget shortfalls

44%

Legacy infrastructure

43%



Complexity of migration

32%

"To me, the people are the most important…all agencies are struggling with this because cyber is changing so quickly"
– Federal cyber leader

Takeaway: Budgets and Legacy Tech Stall Progress

*Respondents asked to select up to three

Preparing for the Future

- Looking ahead, Feds are most concerned about the threat of malware and poor system administration

Which of the following will pose the **greatest overall threat** to your agency's cybersecurity in three to five years?*

#1
Malware (40%)

#2
Poor system administration (including cloud misconfiguration) (32%)

#3
Identity theft (including stolen credentials) (29%)

#4
Malicious insider (25%)

#4
Accidental user error (21%)

#6
Poor patching (19%)

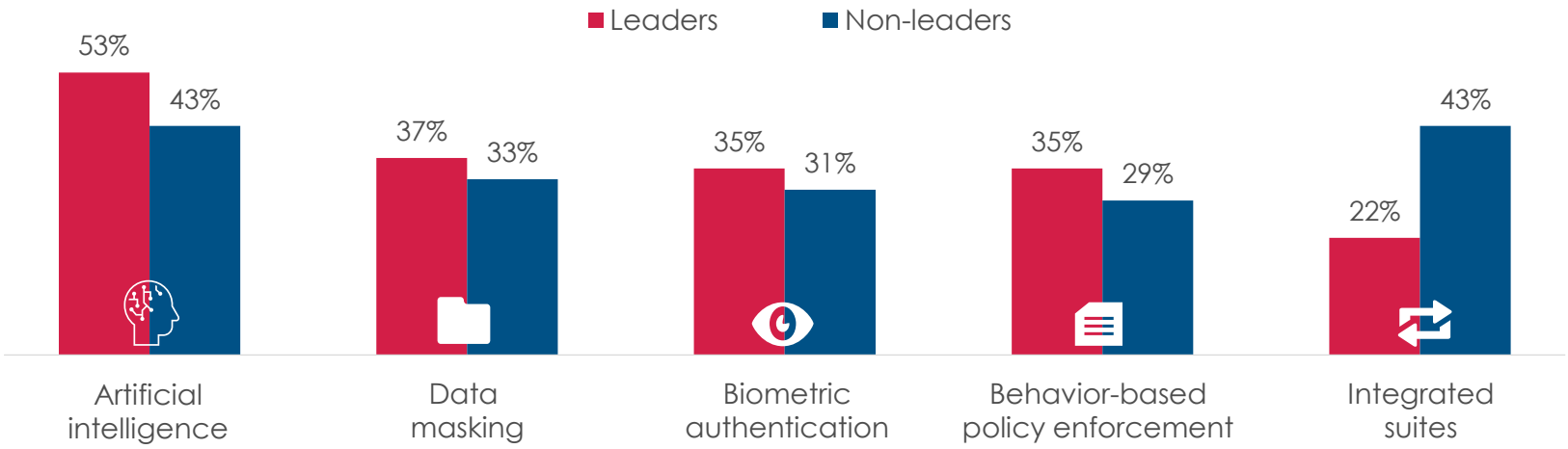
Takeaway: Feds Must Think Inside-Out and Outside-In

*Respondents asked to select up to two

Vital Technologies

- Leaders predict artificial intelligence will be the most valuable addition to their efforts

What innovative security technologies will be most valuable to your agency in three to five years?*



Takeaway: Agreement on AI; Disconnect on Integrated Suites

*Respondents asked to select all that apply

Redesigning Federal Cybersecurity

MeriTalk
Improving the Outcomes of Government IT

- If given the chance to rebuild their ideal cyber strategy, Feds would start with a zero-trust model and ensure full-scope visibility into the network

If you could rebuild your cybersecurity today, with no budget or talent restrictions, what would it look like?

"Start with a **zero-trust model** and build out your security requirements from there"

"A mix of **firewalls, biometric screening, and adaptive algorithms** that would err on the side of caution"

"A complete integrated suite of cyberthreat technologies that is both reactive and predictive – and provides **full-scope visibility into the network** as well as individual hosts and applications"

"**Digital transformation** for data in legacy systems and an agency-wide cyber platform with integrated IT management"

"**Real-time reporting solution** supporting all platforms in a cloud environment"

Takeaway: Shared Vision Includes Zero Trust, Visibility, and Agility

Recommendations

Educate and engage senior leadership: Federal cybersecurity leaders take a more disciplined approach to their cyber strategy and executive-level communication. Secure agency buy-in with frequent threat updates and ROI demonstrations.

Stay agile: Federal cyber leaders review, update, and implement their cybersecurity strategy on an ongoing basis. Leverage growing cyber data and dashboard visualizations to adjust priorities in real time.

Align new investments with a modern cyber vision: Federal IT managers agree the ideal cybersecurity strategy is proactive, relying on zero-trust principles and high network visibility. Collaborate across cyber teams to reimagine your ideal system and ensure new investments bring you closer to your goal.

Methodology & Demographics

MeriTalk, on behalf of Forcepoint, conducted an online survey of 150 Federal IT decision makers familiar with their organization's cybersecurity plans in April 2020. The report has a margin of error of ±7.97% at a 95% confidence level.

Respondent job titles

C-suite or executive-level IT decision maker	17%
IT director/supervisor	44%
Cybersecurity or network director/supervisor	11%
IT specialist	10%
IT engineer or systems/applications architect	5%
Computer/data scientist	3%
IT analyst	5%
Other IT manager	5%

Agency

Federal government: Civilian organization	56%
Federal government: DoD or Intel organization	44%

Expertise

100% of qualifying Federal IT decision makers are familiar with their agency's cybersecurity plans

Thank You

www.meritalk.com

report@meritalk.com

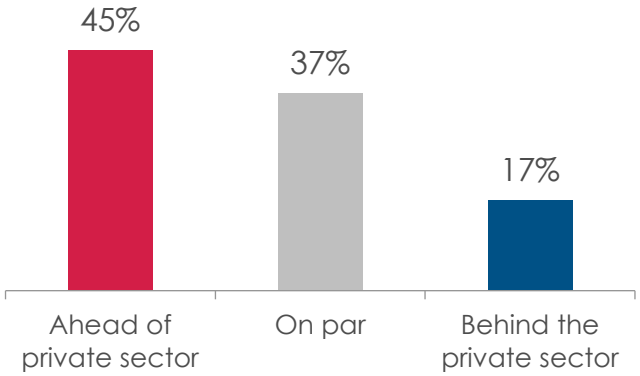
703-883-9000 ext. 164

Appendix: Federal Government vs. Private Sector Results

In November 2019, WSJ Intelligence conducted a similar survey of global private sector CEOs and CISOs. The following slides highlight notable differences between the results of the two studies, both underwritten by Forcepoint

Comparison to Private Sector

Federal IT Managers: Is the Federal government ahead or behind the private sector in cybersecurity?*



75% of Feds say they look to the private sector for guidance when determining their cybersecurity strategy

Strategy comparison

58% of U.S. CEOs and CISOs say cybersecurity is a **top priority** in their organization vs. just **39%** of Feds

Private sector cyber strategies are also significantly closer to their ideal strategy – **27%** of U.S. CEOs and CISOs say they're identical vs. just **11%** of Feds

Innovative tech's impact on cybersecurity

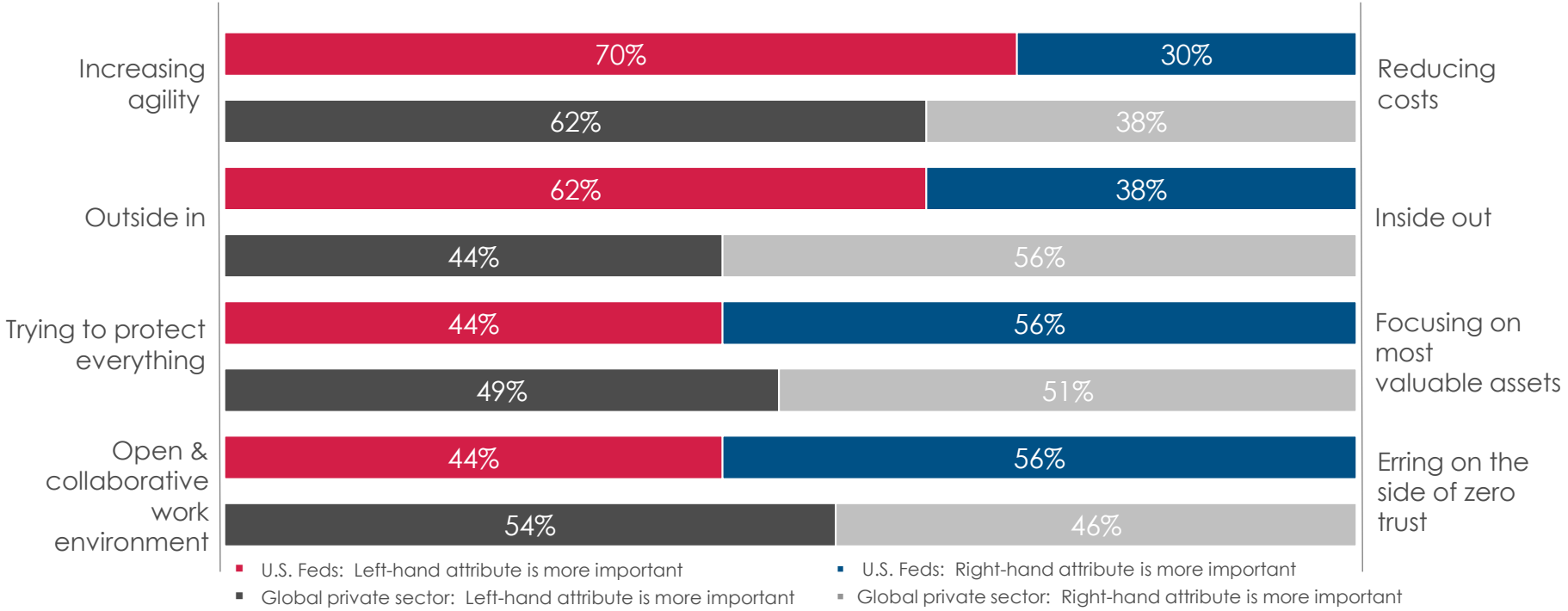
Only **33%** of global private-sector cyber leaders see value in AI for cyber initiatives, compared to **53%** of Federal leaders

Conversely, **56%** see value in behavior-based policy enforcement, compared to **35%** of Federal leaders

*The remaining 1% is unsure

Current Strategy – Feds vs. Private Sector

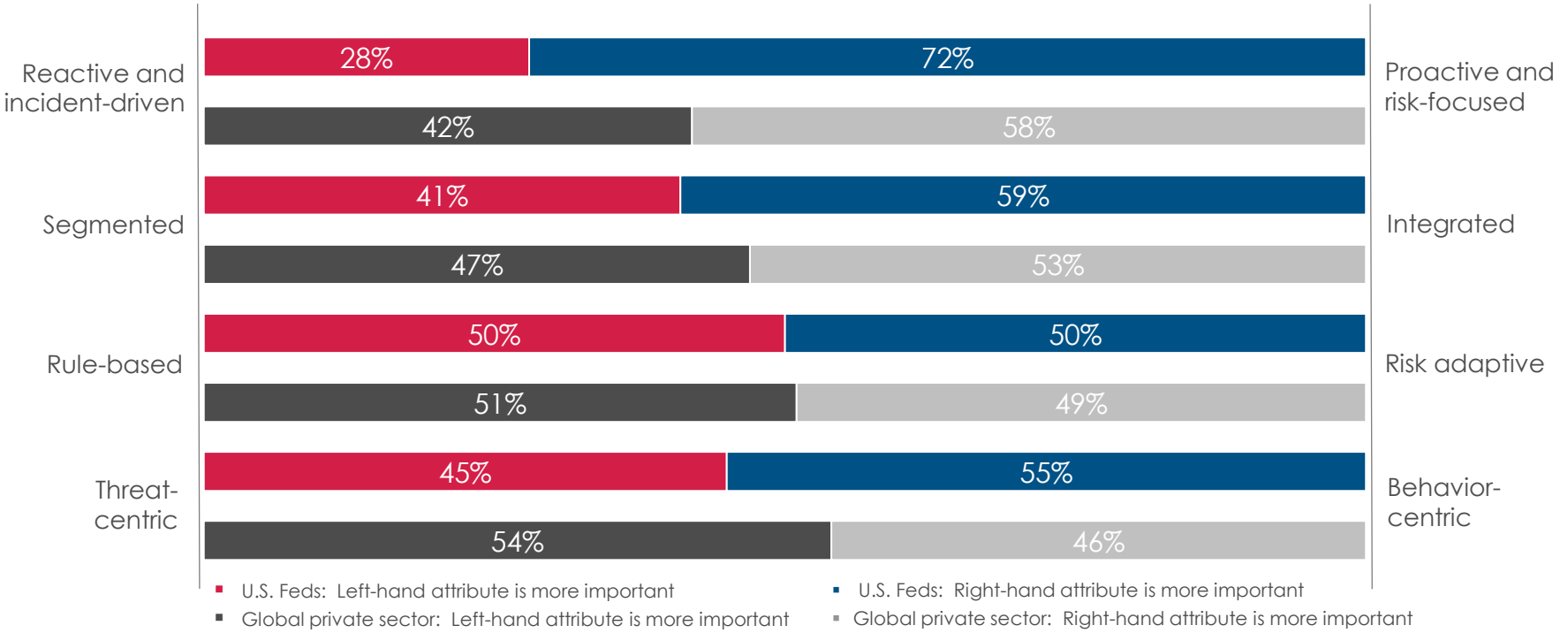
Where is your current strategy positioned across the following dimensions?*



*Does not include percentage who said these are equally important; Only includes comparable dimensions. "More important" combines somewhat and much more important

Ideal Strategy – Feds vs. Private Sector

Where is your ideal strategy positioned across the following dimensions?*



*Does not include percentage who said these are equally important. "More important" combines somewhat and much more important