MeriTalk
Improving the Outcomes of Government IT

merlin cyber

Zeroing In:

2022 State of Federal Zero Trust Maturity

Introduction

With cybersecurity breaches on the rise and clear marching orders from the 2021 Cybersecurity Executive Order[1], Federal agencies are zeroed in on **zero trust**.

What impacts are initiatives like OMB's Federal Zero Trust Strategy[2] and CISA's Zero Trust Maturity Model[3] having on agency efforts? Which zero trust pillars are taking precedence, and which are falling behind? Importantly, what roadblocks continue to hold back agency progress?

MeriTalk and Merlin Cyber surveyed **151 Federal cybersecurity decision-makers** to explore:

- Momentum, priorities, and challenges around zero trust
- Feasibility across each of the five pillars
- Significant differences between Federal civilian and Department of Defense (DoD) perspectives

[1] *Executive Order on Improving the Nation's Cybersecurity*
[2] *Office of Management and Budget's Federal Strategy For a Zero Trust Architecture*
[3] *Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model*

Executive Summary

Federal agencies got the memo – zero trust is a top priority:

73% of Federal cybersecurity decision-makers report their agency is **aggressively adopting** zero trust principles; another **26%** are adopting where they feel it makes sense

92% say recent initiatives such as the EO, OMB's strategy, and CISA's maturity model have increased their confidence in their agency's ability to implement zero trust

But many are concerned about the feasibility of Federal zero trust goals:

87% feel the EO/OMB pushes agencies to move too fast for effective zero trust implementation

When it comes to the pillars of zero trust, **three out of four** say reaching optimum maturity will be a challenge – particularly within the Device and Network pillars

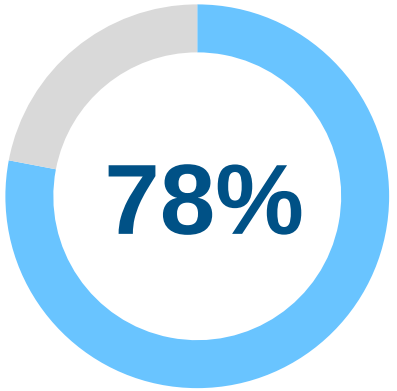
Agencies see goals involving **automation**, **visibility**, and **governance** as most daunting

Public-private partnerships will be key to success:

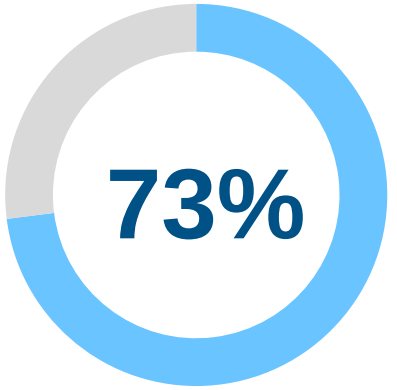
Approximately **one in ten** feel they have the support they need to achieve optimal zero trust maturity, with nearly all seeking vendor guidance and Federal government training

Agencies say they'll need the most help with tool **consolidation**, legacy **integration**, and continued zero trust **education**

Urgency of Zero Trust



of Federal cybersecurity decision-makers feel a **strong sense of urgency** for implementing a zero trust architecture



report their agency is **aggressively adopting** zero trust principles; another 26% are adopting where they feel it makes sense

TAKEAWAY:

Federal agencies are prioritizing zero trust

Juggling Expectations

92%

say recent **Federal initiatives** such as the EO, OMB's strategy, and CISA's maturity model have increased their **confidence** in the implementation of zero trust

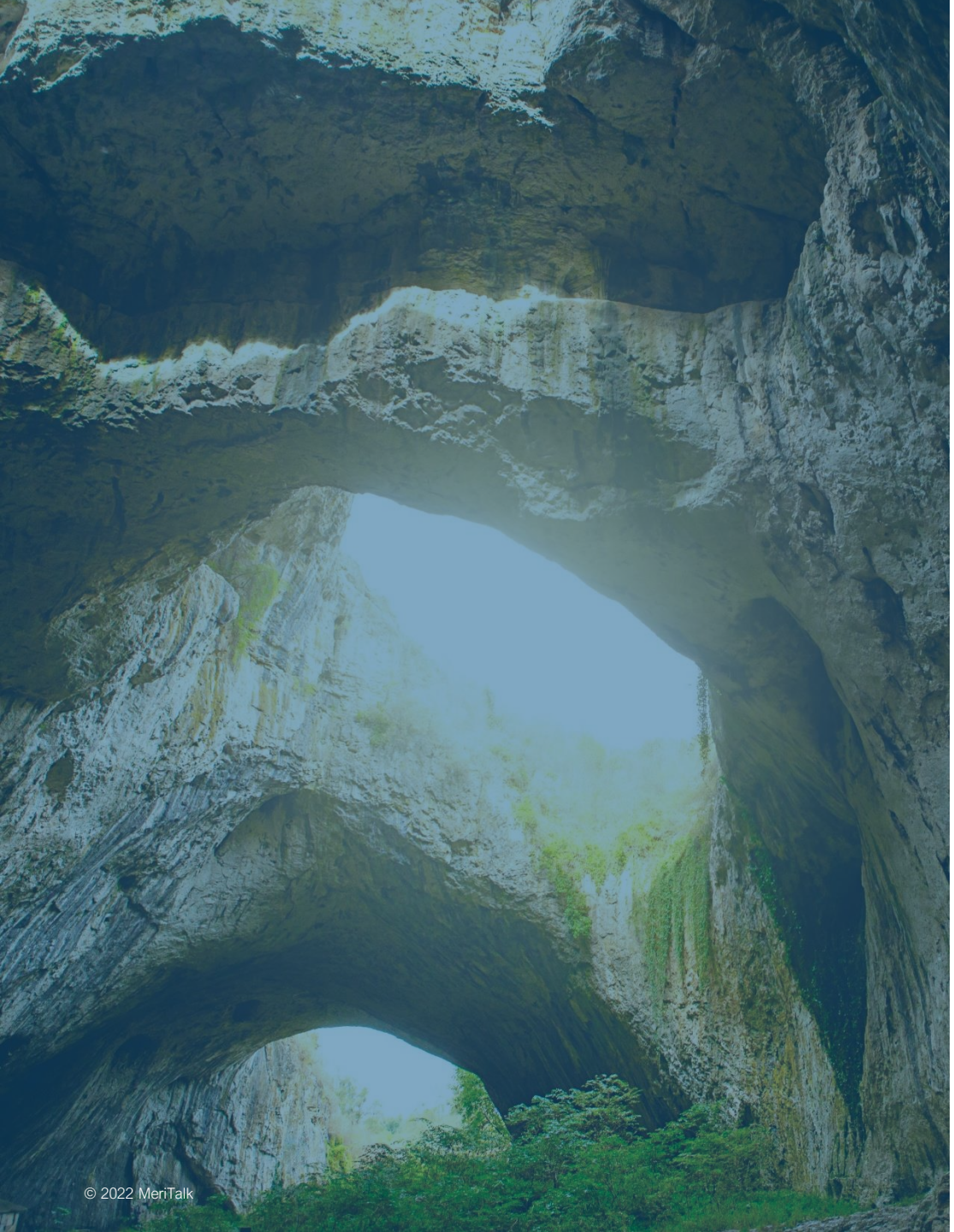
But

87%

feel the EO/OMB pushes agencies to move **too fast** for effective zero trust implementation

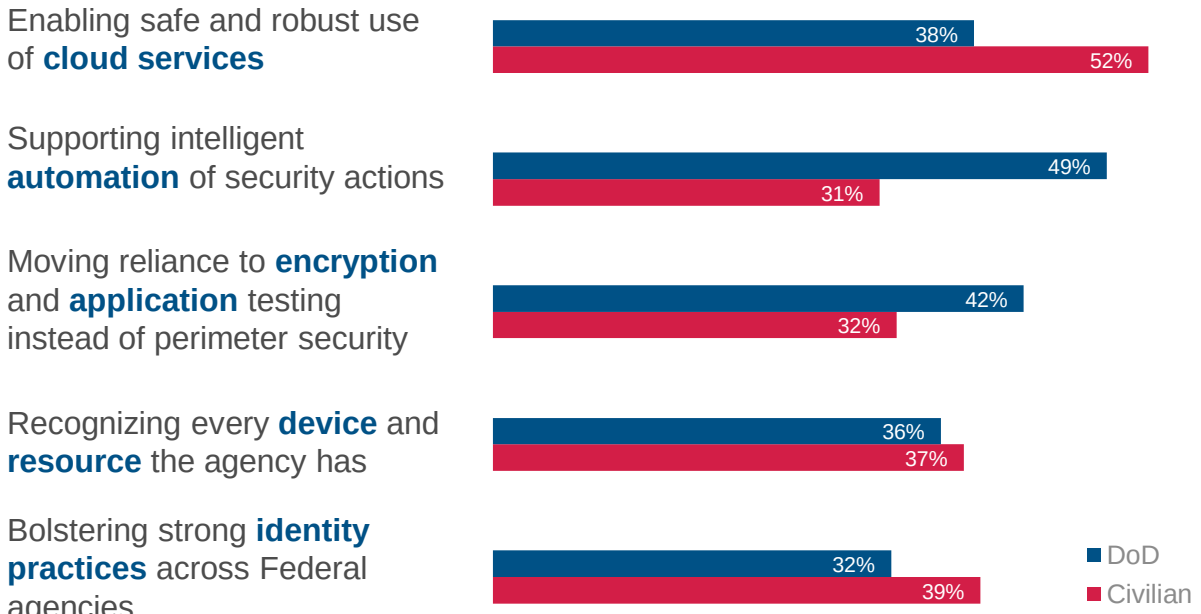
TAKEAWAY:

Federal roadmaps are vital, but may be overly optimistic



Zero Trust Goals

Which of the following **zero trust goals** are most important to your agency?*

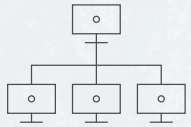


DoD agencies are significantly more likely than civilian agencies to **prioritize intelligent automation**

*Respondents asked to select the top two

Expected Challenges

What **difficulties** do you see your agency facing while implementing a zero trust architecture?*



Centralizing previously siloed cybersecurity tools/deployments (**DoD 45%**, **Civ 44%**)

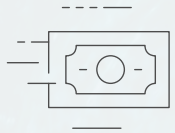
Integrating new solutions with legacy systems that rely on implicit trust (**DoD 42%**, **Civ 43%**)

Staffing/training the IT workforce (**DoD 41%**, **Civ 43%**)

Selecting the right vendor solution(s) (**DoD 42%**, **Civ 36%**)

Training the non-IT workforce (**DoD 32%**, **Civ 41%**)

Juggling competing priorities like zero trust adoption and daily operations (**DoD 39%**, **Civ 33%**)



Budgeting for new software/hardware (**DoD 41%**, **Civ 29%**)

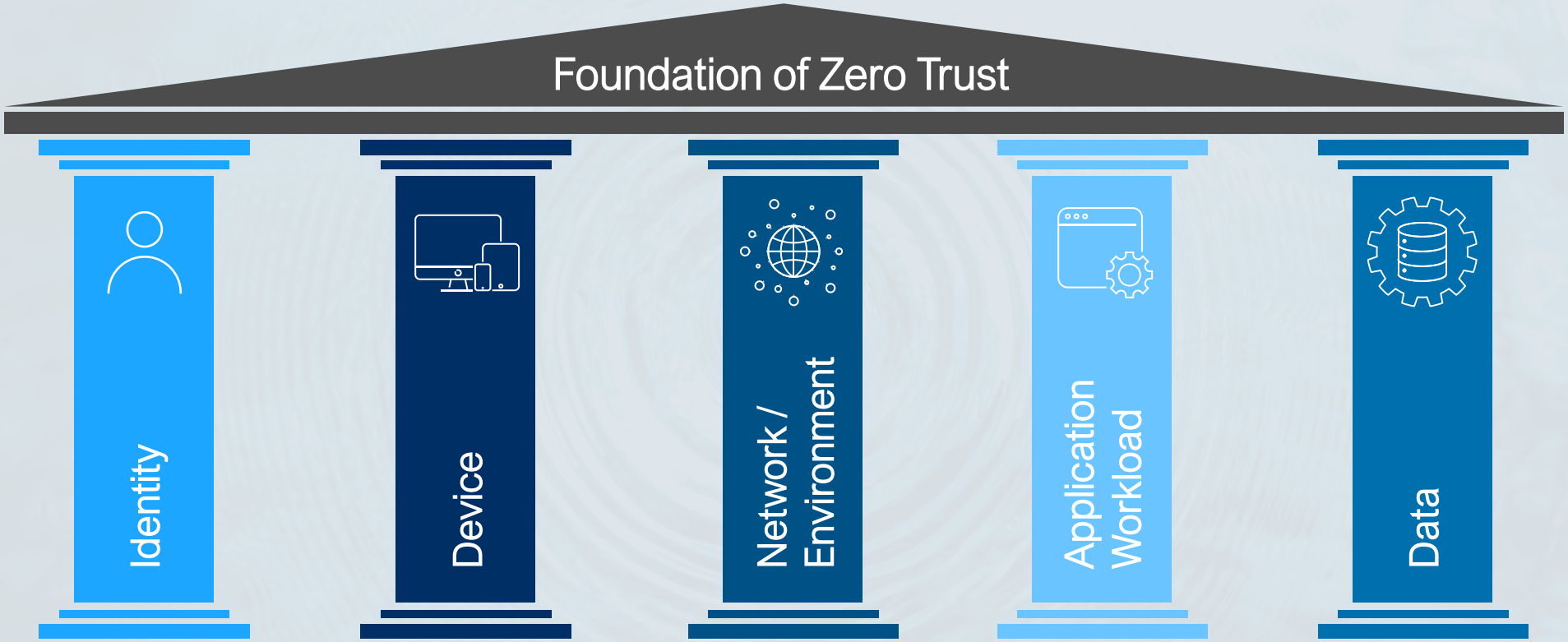
Addressing FedRAMP requirements (**DoD 28%**, **Civ 32%**)

*Respondents asked to select all that apply

TAKEAWAY:

Top challenges center on integration & education

A Closer Look: The Zero Trust Pillars



OMB's FY24 zero trust goals

- Enterprise-wide identity
- Phishing-resistant MFA

- Inventory of every device operated and authorized
- Respond to incidents on those devices

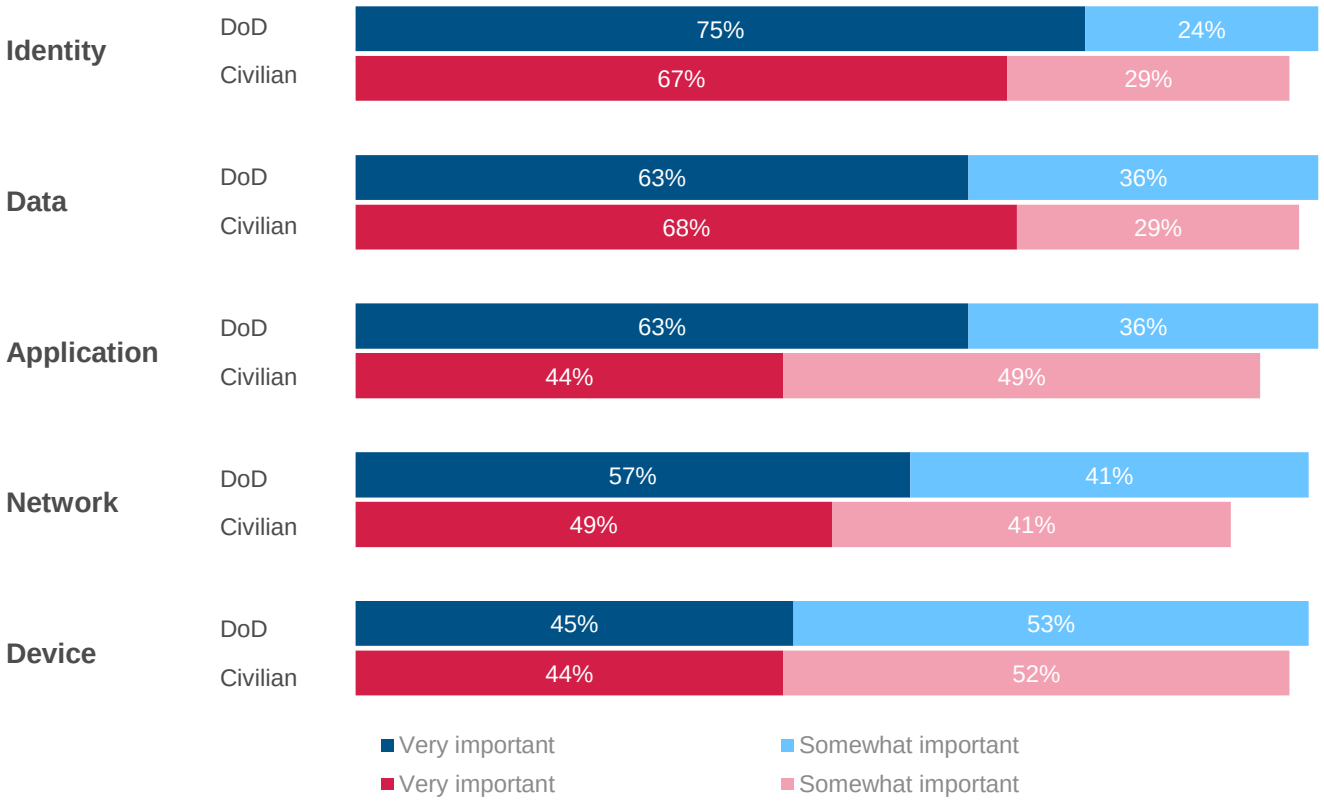
- Encrypt all DNS requests/HTTP traffic
- Segment networks
- Encrypt email in transit

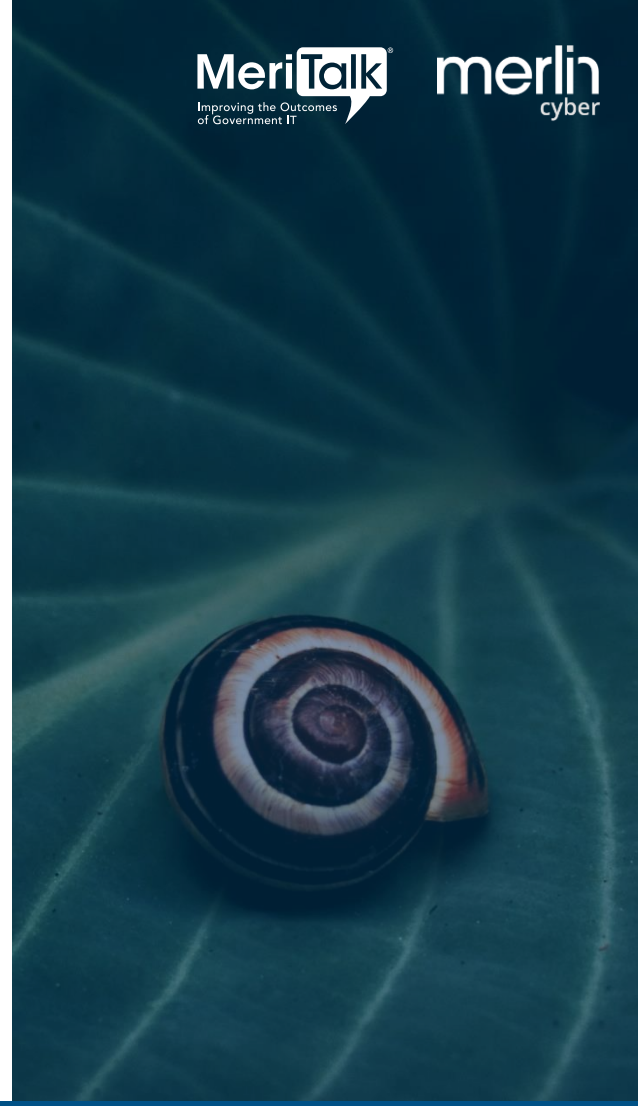
- Treat all applications as internet-connected
- Subject applications to rigorous testing
- External vulnerability reports

- Protections use thorough data categorization
- Cloud security services monitor sensitive data access
- Enterprise-wide logging and information sharing

Prioritizing the Pillars

How **important** are each of the five pillars in OMB's Federal Zero Trust Strategy to your agency's cybersecurity?*





DoD agencies are significantly more likely than civilian agencies to see the **Application pillar** as very important

*Remaining respondents said not very or not at all important

Order of Implementation

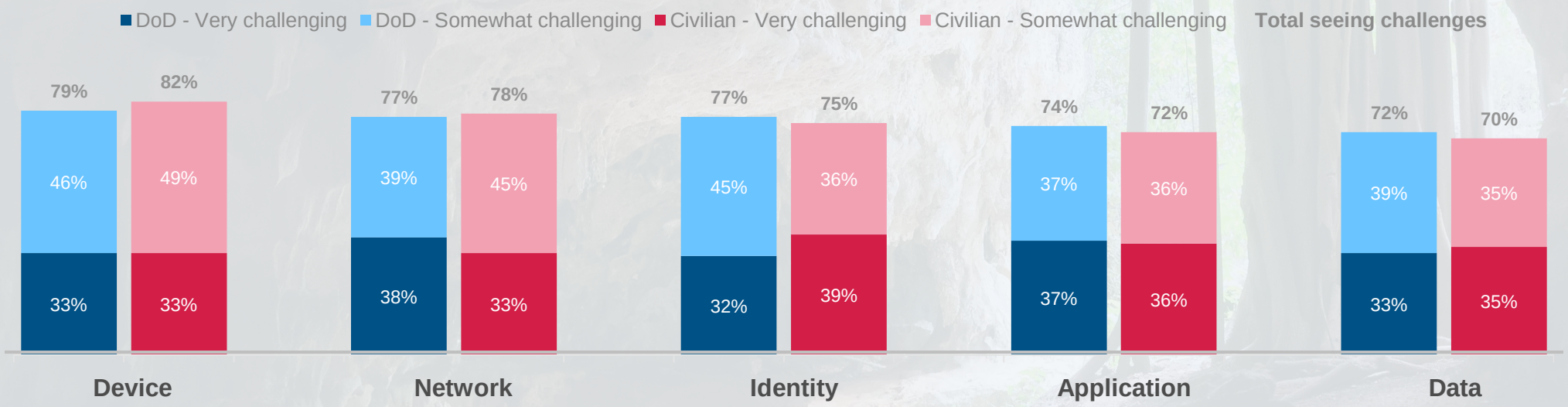
When it comes to the order of **implementation**, a plurality of agencies will start with the Identity pillar:

Order	1st	2nd	3rd	4th	5th
DoD					
Identity	38%				
Device		21%	22%	24%	
Network	24%		24%		
Application				29%	30%
Data		30%			32%
Civilian					
Identity	40%				
Device		24%	29%		
Network			24%	27%	
Application				32%	
Data					41%

DoD agencies are significantly more likely than civilian agencies to begin with the **Network pillar**

Degree of Difficulty

How challenging will it be for your agency to reach **optimal maturity** for each of the five pillars?*



(defined by CISA as: constant device security monitoring and validation; data access depends on real-time risk analytics)

(defined by CISA as: fully distributed ingress/egress micro-perimeters; machine learning-based threat protection; all traffic is encrypted)

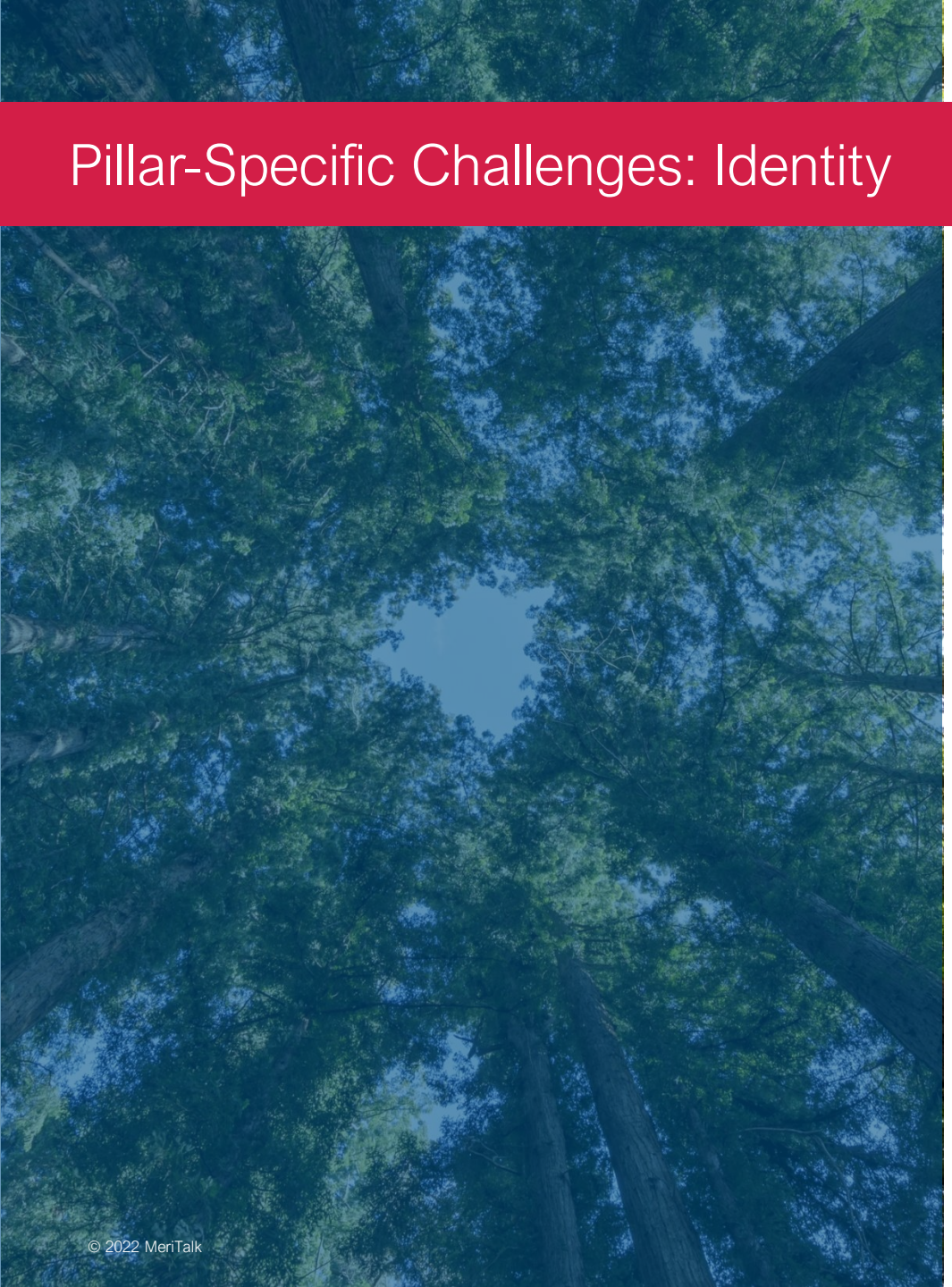
(defined by CISA as: continuous validation; real-time machine learning analytics)

(defined by CISA as: access is authorized continuously, strong integration into application workflow)

(defined by CISA as: dynamic support, all data is encrypted)

*Remaining respondents said not very, not at all challenging, or unsure

Pillar-Specific Challenges: Identity



Which **Identity goals** will be most challenging?*

Visibility and analytics capability – Agency centralizes user visibility with high fidelity attributes along with user and entity behavior analytics (UEBA)

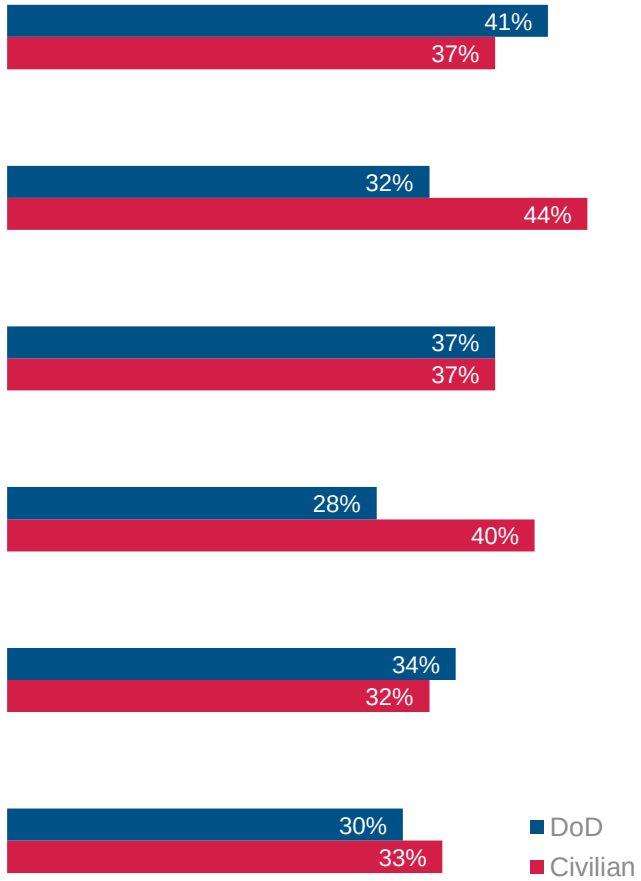
Authentication – Agency continuously validates identity, not just when access is initially granted

Automation and orchestration capability – Agency fully orchestrates the identity lifecycle; implements dynamic user profiling, dynamic identity and group membership, and just-in-time/just-enough access controls

Risk assessment – Agency analyzes user behavior in real time with machine learning algorithms to determine risk and deliver ongoing protection

Identity stores – Agency has global identity awareness across cloud and on-premises environments

Governance capability – Agency fully automates technical enforcement of policies; updates policies to reflect new orchestration options



*Percentage who see the goal as very challenging

Pillar-Specific Challenges: Device

Which **Device goals** will be most challenging?*

Automation and orchestration capability – Agency's device capacity and deployment uses continuous integration and continuous deployment (CI/CD) principles with dynamic scaling

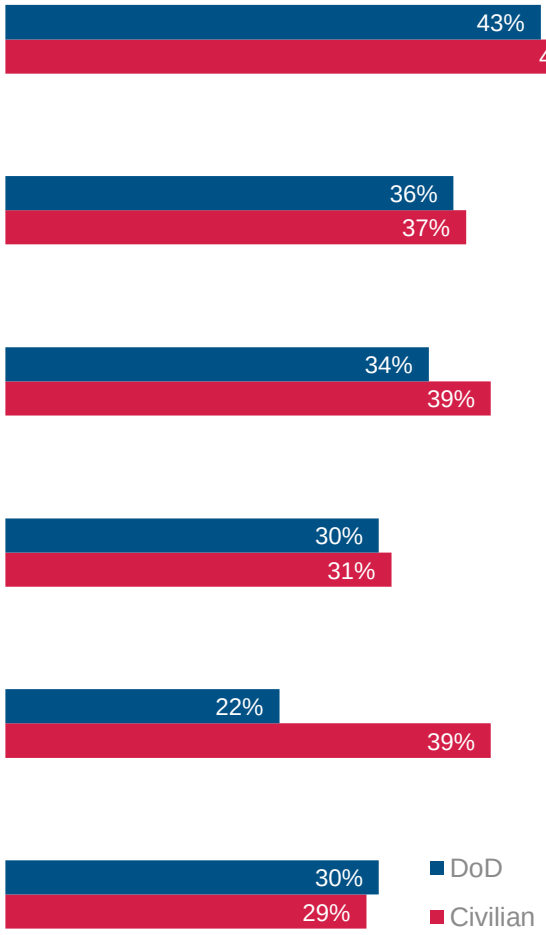
Governance capability – Agency devices permit data access and use without resident plain-text copies, reducing asset supply chain risks

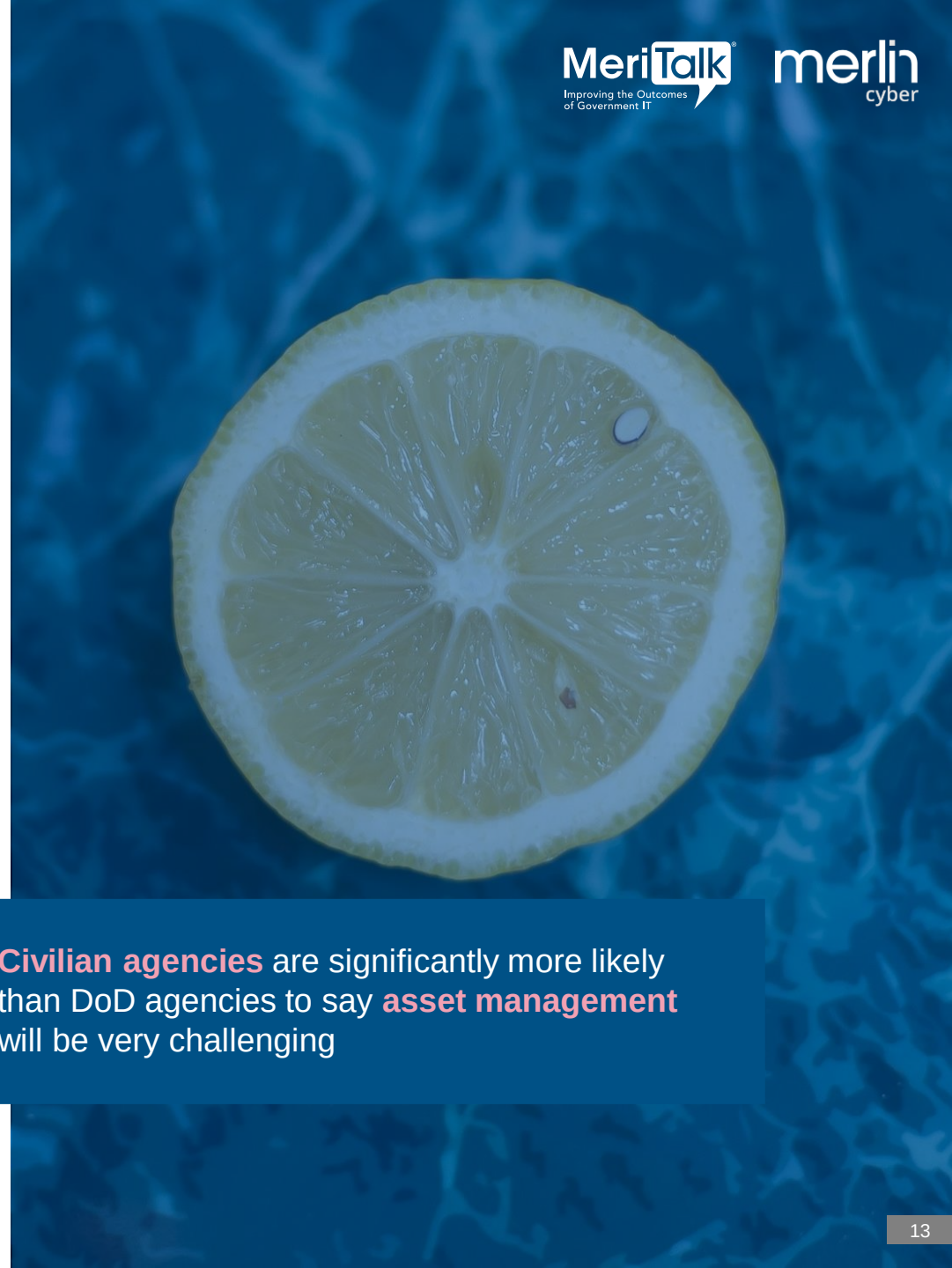
Compliance monitoring – Agency constantly monitors and validates device security posture

Visibility and analytics capability – Agency continuously runs device posture assessments (e.g., using endpoint detection and response (EDR) tools)

Asset management – Agency integrates asset and vulnerability management across all agency environments, including cloud and remote

Data access – Agency's access to data considers real-time risk analytics about devices





Civilian agencies are significantly more likely than DoD agencies to say **asset management** will be very challenging

*Percentage who see the goal as very challenging

Pillar-Specific Challenges: Network

Which **Network goals** will be most challenging?*

Threat protection – Agency integrates machine learning-based threat protection and filtering with context-based signals

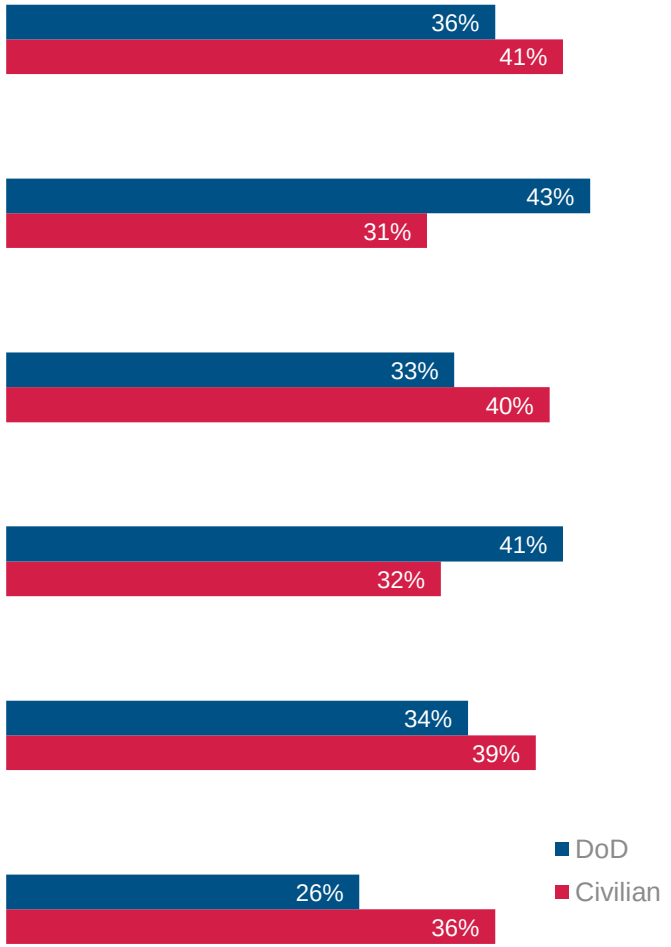
Encryption – Agency encrypts all traffic to internal and external locations, where possible

Automation and orchestration capability – Agency network and environment configurations use infrastructure-as-code, with pervasive automation, following CI/CD deployment models

Governance capability – Agency uses automated discovery of networks, devices, and services, with manual or dynamic authorization and automated remediation of unauthorized entities

Visibility and analytics capability – Agency integrates analysis across multiple sensor types and positions with automated alerts and triggers

Network segmentation – Network architecture consists of fully distributed ingress/egress micro-perimeters and deeper internal micro-segmentation based around application workflows



*Percentage who see the goal as very challenging

Pillar-Specific Challenges: Application

Which **Application goals** will be most challenging?*

Application security – Integrates application security testing throughout the development and deployment process, with regular automated testing of deployed applications

Visibility and analytics capability – Agency performs continuous and dynamic application health and security monitoring with external sensors and systems

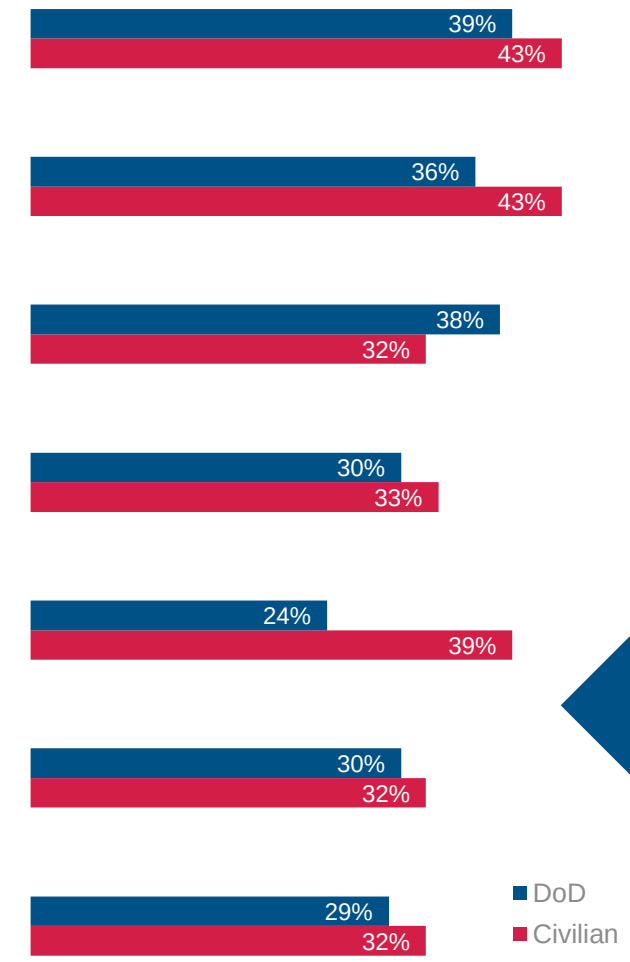
Access authorization – Agency continuously authorizes access to applications, considering real-time risk analytics

Threat protections – Agency strongly integrates threat protections into application workflows, with analytics to provide protections that understand and account for application behavior

Governance capability – Agency has updated policies and dynamic enforcement

Accessibility – All applications are directly accessible to users over the internet

Automation and orchestration capability – Applications adapt to ongoing environmental changes for security and performance optimization



Civilian agencies are significantly more likely than DoD agencies to say the **governance capability** will be very challenging

*Percentage who see the goal as very challenging

*Percentage who see the goal as very challenging

Pillar-Specific Challenges: Data

Which **Data goals** will be most challenging?*

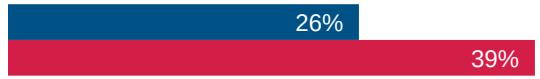
Inventory management – Agency continuously inventories data with robust tagging and tracking, augments categorization with machine learning models

Governance capability – Agency automatically enforces data protections required; uses a unified approach that integrates data (independent of source) to categorize data and authorize access

Access determination – Agency's access to data is dynamic, supporting just-in-time and just-enough principles, and continual risk-based determinations

Automation and orchestration capability – Agency automatically enforces strict access controls for high-value data; all high-value data is backed up regardless of storage location and data inventories are automatically updated

Visibility and analytics capability – Agency's data are inventoried and can always be accounted for; agency logs and analyzes all access for suspicious behaviors and performs analytics on encrypted data



Encryption – Agency encrypts all data at rest

*Percentage who see the goal as very challenging

Agencies Need Help

For Federal cybersecurity decision-makers, **12%** or fewer feel they have all the support they need to achieve optimal maturity for each of the five pillars:

	Defense*	Civilian*
Identity	3%	11%
Device	12%	9%
Network	9%	9%
Application	7%	5%
Data	4%	8%

*Percentage who say they have all the support they need for the pillar

95% of DoD and **92% of Civilian** agencies are looking for **vendor support** for at least one pillar

88% of DoD and **88% of Civilian** agencies are looking for Federal government **training**

TAKEAWAY:

Public-private partnerships are key to zero trust success

How Federal Officials Can Strengthen Support

What is **one thing** Federal officials can provide to help your agency implement zero trust?

> *Support and documentation on **better practices** for implementing zero trust technology"*

> *More cutting-edge high-tech **technical personnel**"*

> ***Certifications** that can be based on globally recognized technical practices"*

> *Professional **education and training** as well as the implementation of more advanced automation tools"*

> *Highly attributed **centralized user visibility**, secure monitoring, and verification of stable devices"*

> ***Simple structure**, convenient maintenance, improve cost effectiveness"*

Recommendations

Capitalize on Confidence

The energy around zero trust is palpable with 73% of Federal cybersecurity decision-makers reporting their agency is aggressively adopting zero trust principles per the White House's May 2021 mandate.

While many have concerns about the feasibility of OMB's FY24 goals, they feel the collective guidance from the EO, OMB, and CISA has increased their confidence in their agency's ability to implement a zero trust architecture.

Agencies should continue to capitalize on this momentum by reallocating resources and minimizing competing priorities to rally cyber teams around this singular, shared purpose.

Prioritize the Pillars

While high-level support for zero trust is at a fever pitch, more than 70% of agencies still doubt their ability to reach optimum maturity in each of the architecture's five pillars.

Agencies understand identity systems are at the foundation of zero trust, but beyond that, approaches and timelines vary.

Agencies need support – especially around the Network and Data pillars. The next round of Federal guidance must provide a detailed roadmap for the next leg of the journey, including pillar prioritization and comprehensive implementation instructions. It should offer agencies suggestions to customize for their needs, either alone or with aid from the private sector.

Automate and Integrate

As cyber decision-makers think ahead to optimal zero trust maturity, some of the most daunting goals center on visibility and and automation.

While agencies can't modernize legacy systems overnight, cloud solutions may help bridge the gap. Consider solutions with baked-in zero trust principles like centralized visibility, auto-enforced access controls, and continuous monitoring and integration.

Public-private sector collaboration will be essential as agencies move from zero trust confidence to competence over the next three years.

Methodology

Respondent job titles

C-Suite	18%
IT Director/Supervisor	44%
Cybersecurity Program Manager/Officer	23%
Software/Applications Development Manager	7%
Data Center or Network Manager	2%
Cybersecurity Specialist/Analyst/Engineer	5%
Other IT Manager	1%

Employer

Federal Government: Civilian Agency	50%
Federal Government: DoD or Intelligence Agency	50%

Expertise

100% of qualifying respondents are familiar with their organization's cybersecurity initiatives, including zero trust strategies. They all also make, contribute, or otherwise influence their organization's purchasing decisions for digital solutions.

MeriTalk conducted an online survey of 151 Federal cybersecurity decision-makers in November and December 2021. The report has a margin of error of ±7.95% at a 95% confidence level.

Thank You

www.meritalk.com

report@meritalk.com