IT INSIGHTS REPORT

THE QUEST FOR ZERO TRUST

Where federal agencies stand. The challenges still ahead.

Government IT leaders share their views on implementing the core capabilities of zero trust, the challenges agencies face in adopting them and opportunities for accelerating adoption.

PRESENTED BY FEDSCOOP

UNDERWRITTEN BY Forcepoint

EXECUTIVE SUMMARY

Federal agencies have been charged with implementing a comprehensive zero-trust cybersecurity strategy as part of a larger White House Executive Order on improving the nation's cybersecurity.

To better understand government leaders' views on implementing zero trust, the challenges agencies face and the opportunities for accelerating adoption, FedScoop surveyed 177 prequalified federal agency leaders and IT decision-makers in May 2022.

The survey looked at where agencies are in the implementation of zero trust security capabilities — and how budget, technical and operational concerns factor into their plans.

KEY FINDINGS

SECURING RESOURCES

Half of civilian agency respondents (52%) — and 56% from defense/intelligence agencies — are confident that federal zero trust mandates will lead to additional resources for security projects from agency leadership. However, nearly half of civilian agency respondents — and nearly 4 in 10 at defense/intelligence agencies — estimate that 7% or more of agency IT budgets for FY 2023 and 2024 will have to be redirected to fully finance the administration's zero trust goals.

MEETING ZERO TRUST GOALS

Less than half of civilian and defense/intelligence agency respondents voiced confidence their agency would achieve OMB's zero trust goals by the end of FY 2024, while 46% in both groups remain skeptical or not confident about meeting the deadline.

INVESTMENT PRIORITIES

Among the five primary zero-trust security pillars outlined in OMB's goals, identity and access controls were getting the highest investment priority over the next fiscal year, followed by investments in network environments, data, devices and application security. Roughly 1 in 4 respondents said foundational, cross-enterprise systems for managing visibility, analytics, automation and orchestration would not be in place before the end of fiscal year 2025 or beyond.

EXECUTIVE SUMMARY

When thinking of the agency/component's current enterprise-wide security capabilities relative to NIST/CISA/DOD recommended practices:

USER TRUST

Roughly 6 in 10 respondents said their agencies were executing on par with peers or at advanced levels with multi-factor authentication and centralized identity management. At the same time, as many as one-third said their agencies are still in the planning stages or laying the foundations for those capabilities. Civilian agencies have further to go than their defense/intelligence counterparts in getting started deploying conditional access controls.

DEVICE TRUST

Civilian agencies appear better able to inventory devices and assets — with 62% of respondents saying they are executing on par with peers, or at advanced levels — compared to 49% of their defense/intelligence counterparts. Just under 6 in 10 respondents in both groups said their EDR systems are executing on par with peers, or at advanced levels, with about one-third still in the planning or early stages of deployment. The responses were similar for device compliance and authentication capabilities.

NETWORK/TRUST

Roughly 4 in 10 respondents at both civilian and defense/intelligent agencies are still getting started deploying network micro-segmentation — and replacing VPNs with zero trust network access. Defense/intelligence respondents reported having more advanced capabilities than did civilian agency respondents (30% vs. 17%) for encrypting data in transit.

APPLICATION TRUST

While 6 in 10 respondents said their agencies have centralized access authorization capabilities — and two-thirds had single sign-on — for applications, at least 3 in 10 are still getting started with dedicated app security testing and continuous authorization to operate tools.

EXECUTIVE SUMMARY

DATA TRUST

While a majority of respondents said their agencies have data encryption and data loss prevention tools in place on par with their peers, more than 1 in 3 respondents said their agencies are still getting started with data tagging and tracking, data inventory and governance, and automated data flow mapping capabilities.

CHALLENGES

Among the top technical challenges agencies face in establishing zero-trust environments, 4 in 10 respondents cited the interdependency and complexity of existing technology, conflicting IT priorities and managing the growth of data.

Half of all respondents said, “balancing the needs for both productivity and security” and inadequate funding were their top operational challenges, followed by insufficient staff expertise and implement zero trust across diverse operational silos.

However, those challenges varied by agency size, as did recommendations for what measures would help agencies most in achieving the White House’s zero-trust goals.

ACHIEVING ZERO-TRUST GOALS

Agencies leaders said what would help them most to achieve the White House’s zero-trust goals would be: “Greater near-term IT funding for zero trust implementation” (44%); “greater opportunities to tap the government’s Technology Modernization Fund (38%); and “greater flexibility to acquire managed IT/security services” (34%). One-third also suggested, “greater leadership support to implement zero-trust across business unit silos.” Responses varied somewhat when broken out by agency size.

WHO WE SURVEYED

FedScoop surveyed **177** prequalified respondents in May 2022.

RESPONDENT BY **TYPE OF EMPLOYEE**	
Federal agency	**78%**
Contractor/system integrator	**22%**

RESPONDENT BY **AGENCY TYPE**	
Civilian	**58%**
Defense/Intelligence	**42%**

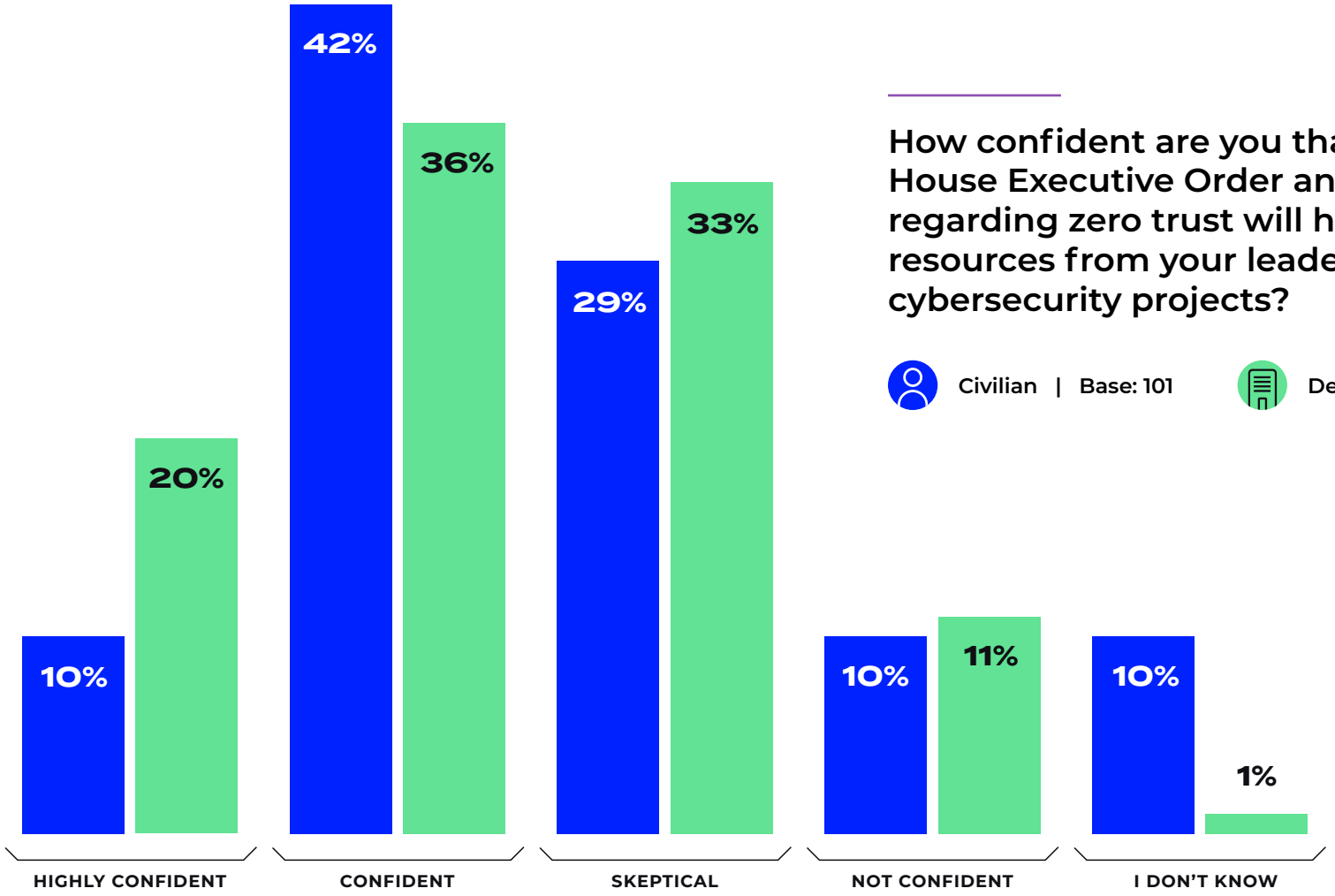
RESPONDENT BY **AGENCY SIZE**	
Less than 5,000 employees	**27%**
5,000 – 10,000 employees	**29%**
More than 10,000 employees	**44%**

RESPONDENT BY **LEVEL OF GOVERNMENT**	
Agency/Department	**65%**
Component/Bureau	**31%**
Other	**4%**

RESPONDENT BY **JOB TITLE**	
C-suite	**11%**
Chief information, technology and security officials	**11%**
IT management	**21%**
IT security management/staff	**12%**
IT influencer	**8%**
Procurement official/staff	**14%**
Other (e.g. program analyst, system engineer)	**23%**

CONFIDENCE FOR ADDITIONAL RESOURCES

Civilian vs. Defense/Intelligence Agencies



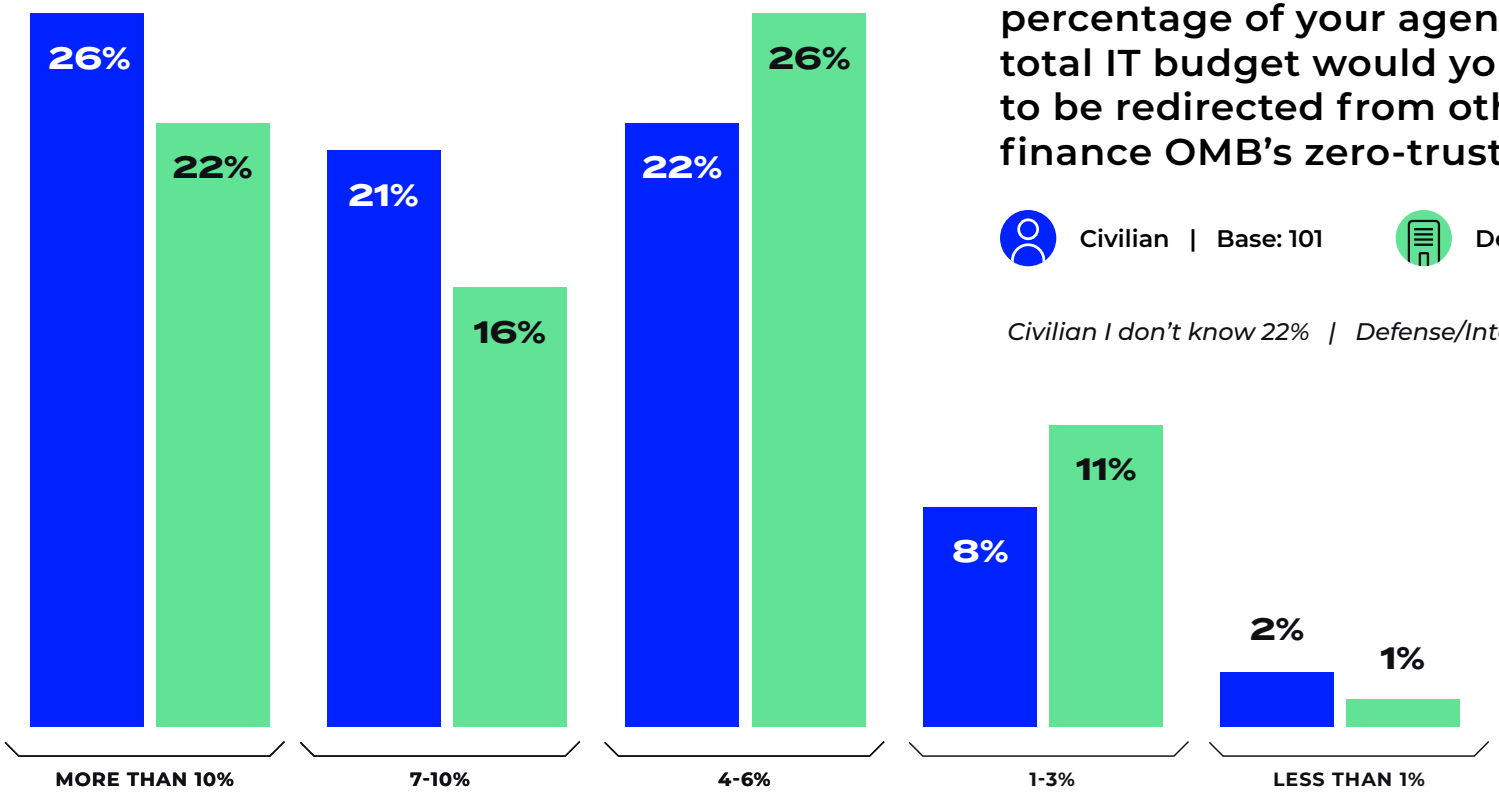
How confident are you that the White House Executive Order and OMB mandates regarding zero trust will help secure additional resources from your leadership toward critical cybersecurity projects?

Civilian | Base: 101

Defense & Intelligence | Base: 76

FINANCING ZERO TRUST REQUIREMENTS

Civilian vs. Defense/Intelligence Agencies



Thinking about FY 2023, roughly what percentage of your agency's/component's total IT budget would you estimate will need to be redirected from other IT projects to finance OMB's zero-trust requirements?

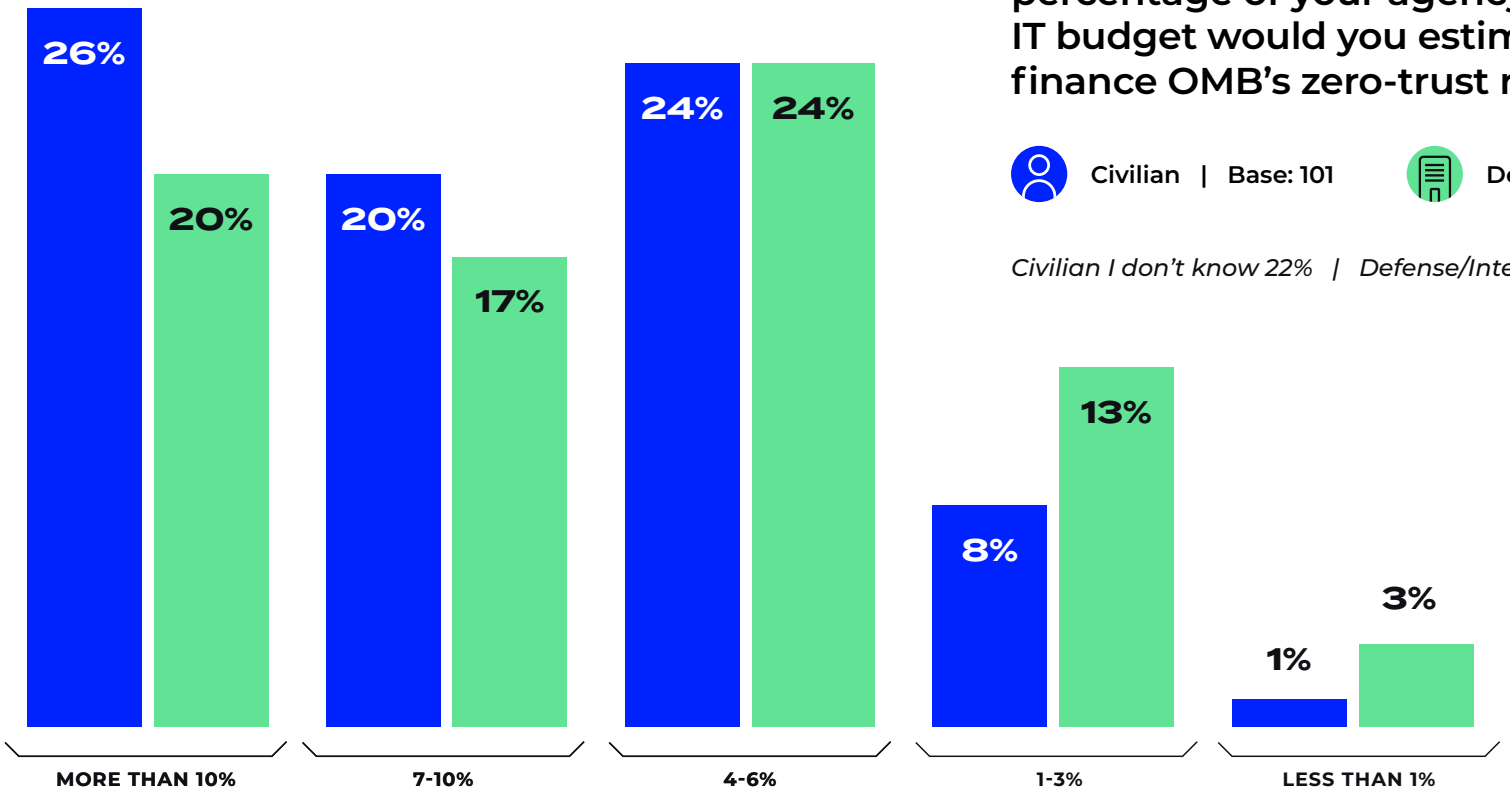
Civilian | Base: 101

Defense & Intelligence | Base: 76

Civilian I don't know 22% | Defense/Intelligence I don't know 24%

FINANCING ZERO TRUST REQUIREMENTS

Civilian vs. Defense/Intelligence Agencies



Thinking about FY 2024, roughly what percentage of your agency's/component's total IT budget would you estimate will be needed to finance OMB's zero-trust requirements?

Civilian | Base: 101

Defense & Intelligence | Base: 76

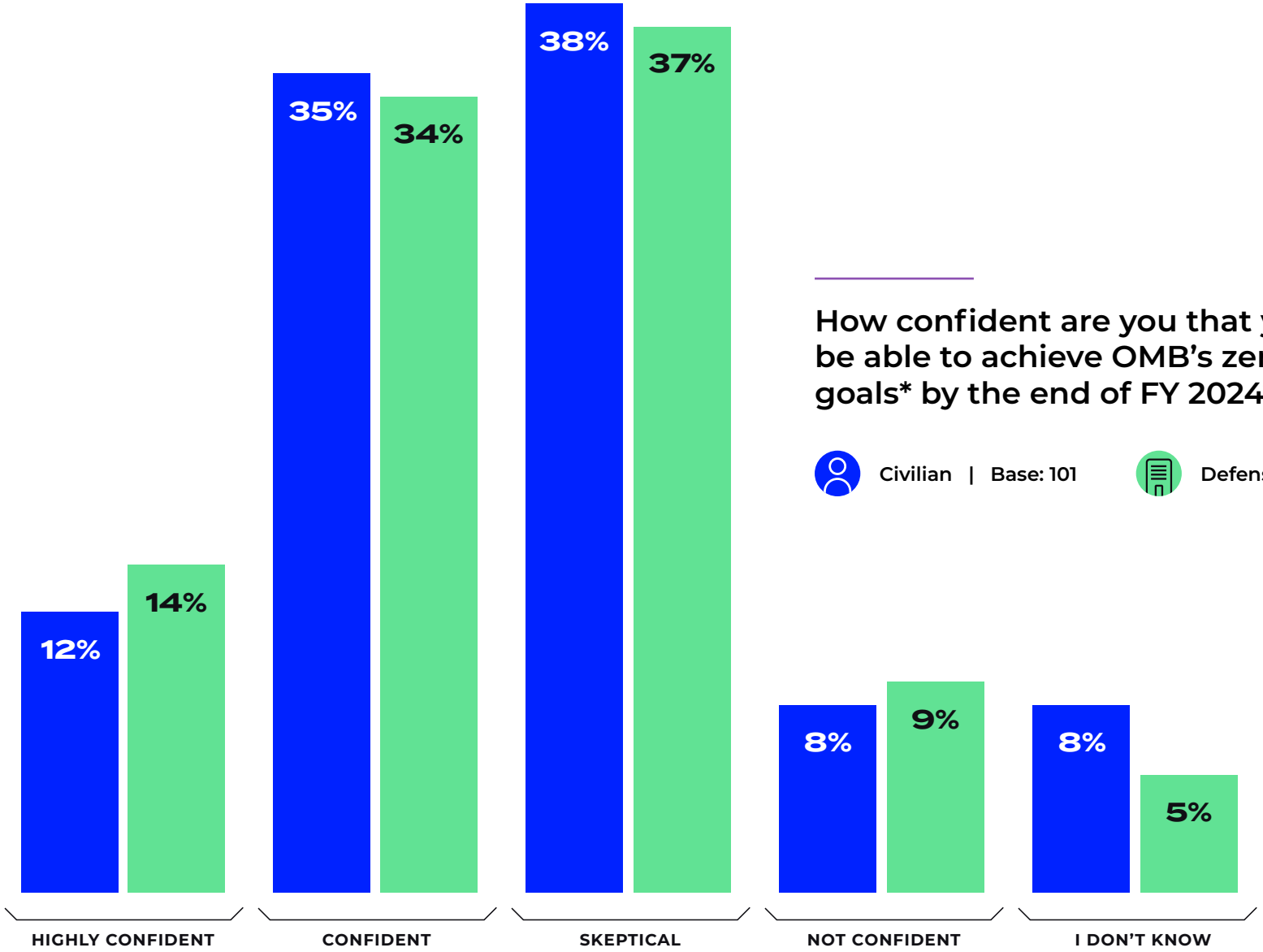
Civilian I don't know 22% | Defense/Intelligence I don't know 24%

OTHER VIEWPOINTS:

When thinking about **FY 2023** and **2024**, a higher percentage of larger-sized agencies believe it will take more than 10% of their agency's IT budget compared to medium and smaller sized agencies.

CONFIDENCE TO MEET ZERO TRUST GOALS FY-END 2024

Civilian vs. Defense/Intelligence Agencies



How confident are you that your agency will be able to achieve OMB's zero trust security goals* by the end of FY 2024?

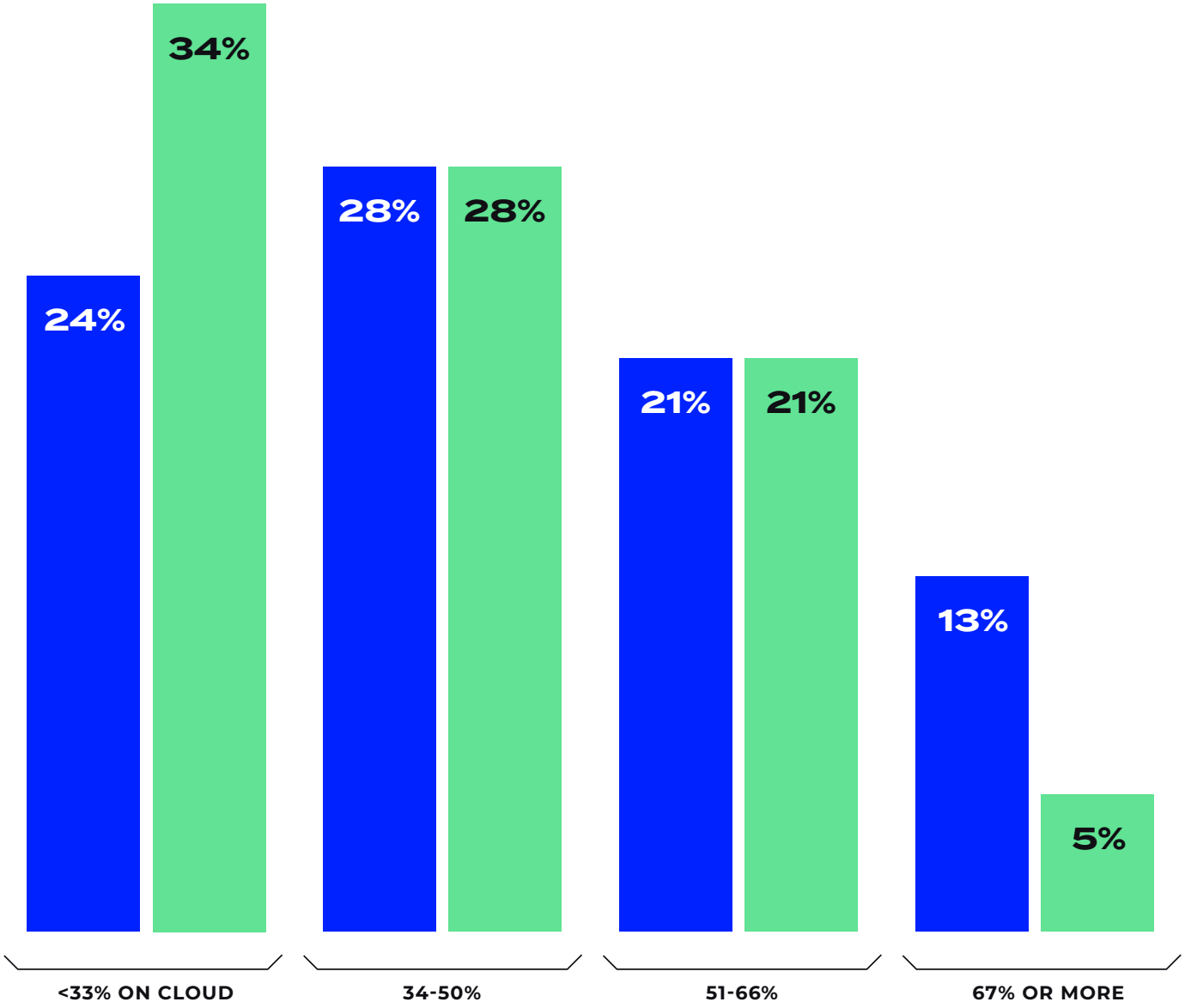
Civilian | Base: 101

Defense & Intelligence | Base: 76

(*Those goals include steps to verify and secure "five pillars" of trust — around users, devices, network traffic, applications and data — and the ability to observe, analyze, automate and orchestrate security measures across those five pillars.)

PERCENTAGE OF WORKLOAD ON CLOUD VS ON-PREM

Civilian vs. Defense/Intelligence Agencies



Zero-trust progress will depend heavily on operating in the cloud. With 24% of civilian agency respondents saying less than one-third of their agency's mission/ operation apps operate in the cloud, implementing all five pillars of zero trust — around users, devices, networks, applications and data — promises to be a challenging endeavor for many federal agencies.

Roughly what percentage of your agency's/component's mission and operations applications currently operate primarily on cloud platforms vs. on-premises?

Civilian | Base: 101

Defense & Intelligence | Base: 76

ZERO TRUST PILLAR PRIORITIES

All respondents

How would you rank your agency's/component's investment priority over the next fiscal year for each zero-trust security pillar?

1st Priority	**IDENTITY AND ACCESS**
2nd Priority	**NETWORK/ENVIRONMENT**
3rd Priority	**DATA**

Base: 177

OTHER PRIORITIES:

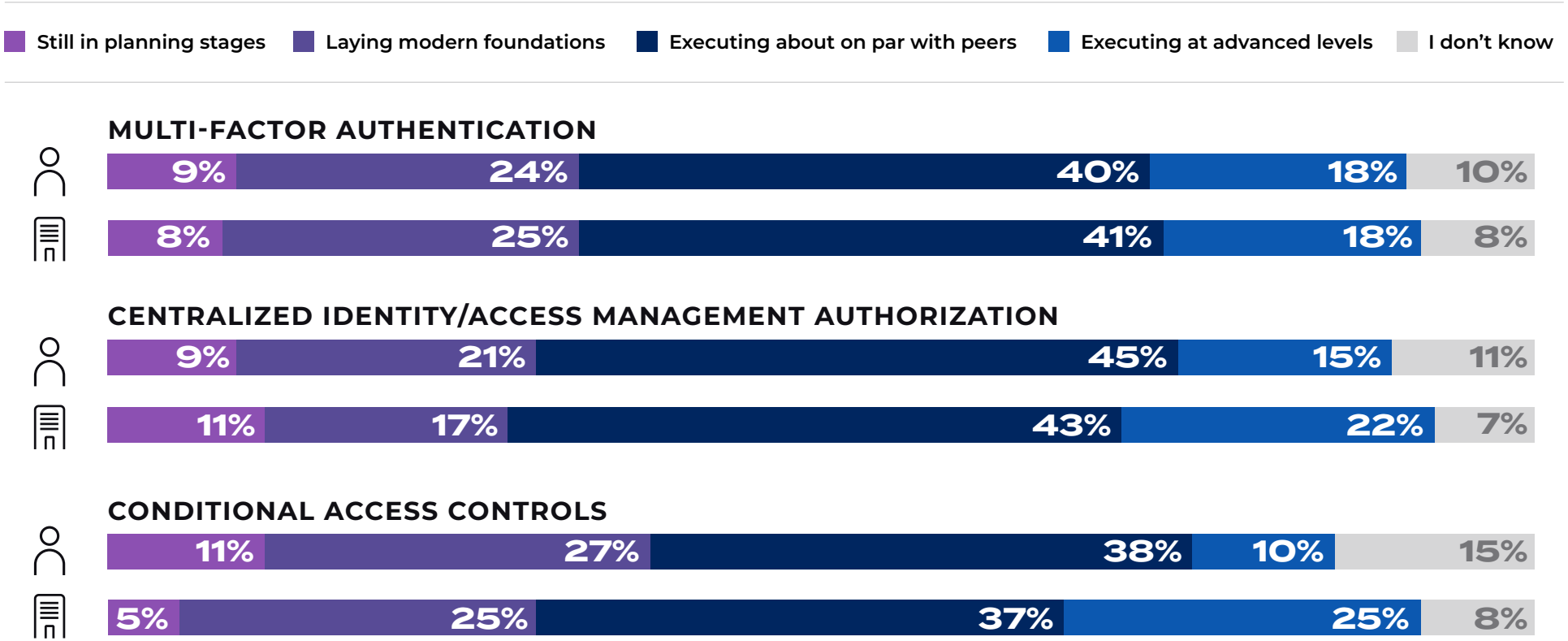
When analyzing how the other zero trust pillars were ranked by all respondents, **devices came in fourth** and **application workload came in fifth** and **lastly was "visibility/analytics/automation/orchestration**."

SECURITY CAPABILITIES

Civilian vs. Defense/Intelligence Agencies

Thinking about your agency's/component's present enterprise-wide security capabilities relative to NIST / CISA / DOD recommended practices:

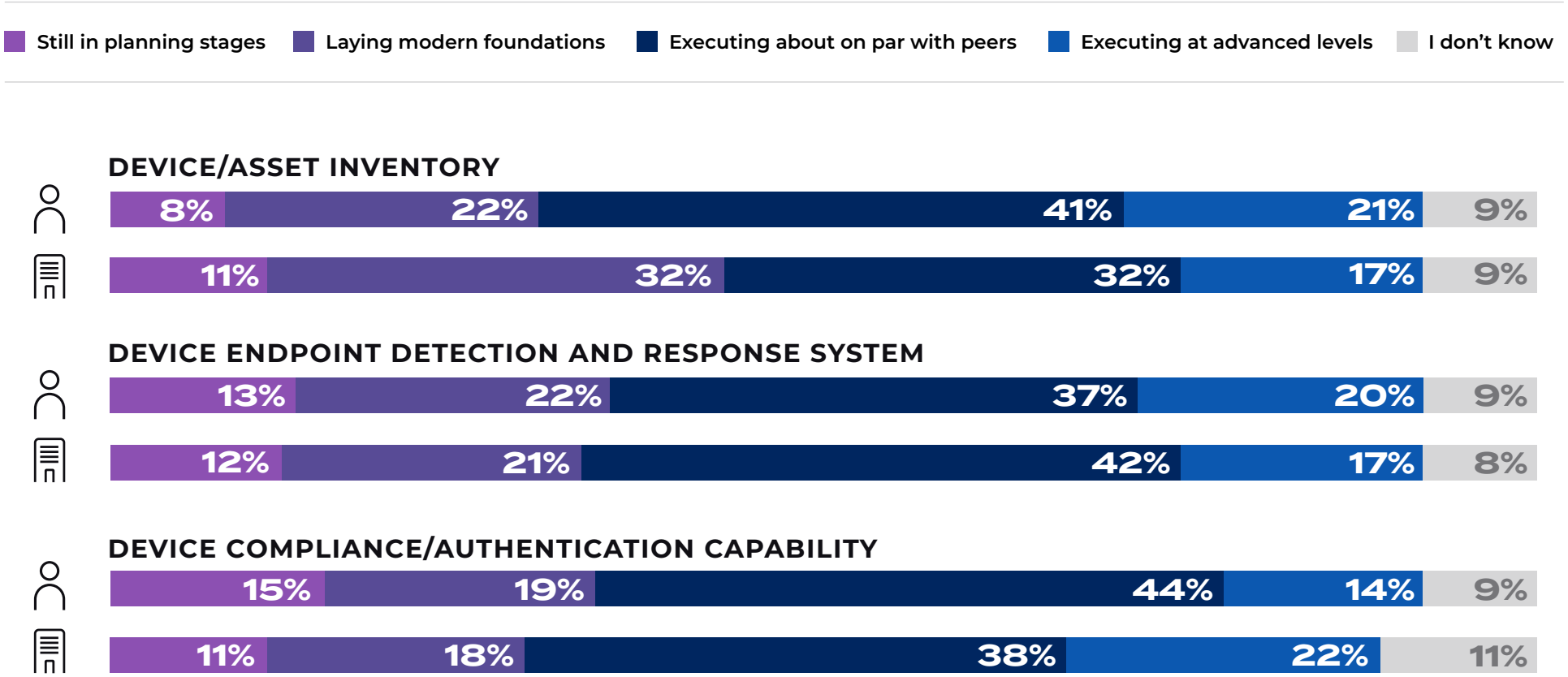
How would security experts likely describe where your agency/component is for USER TRUST?



SECURITY CAPABILITIES

Civilian vs. Defense/Intelligence Agencies

How would security experts likely describe where your agency/component is for DEVICE TRUST?



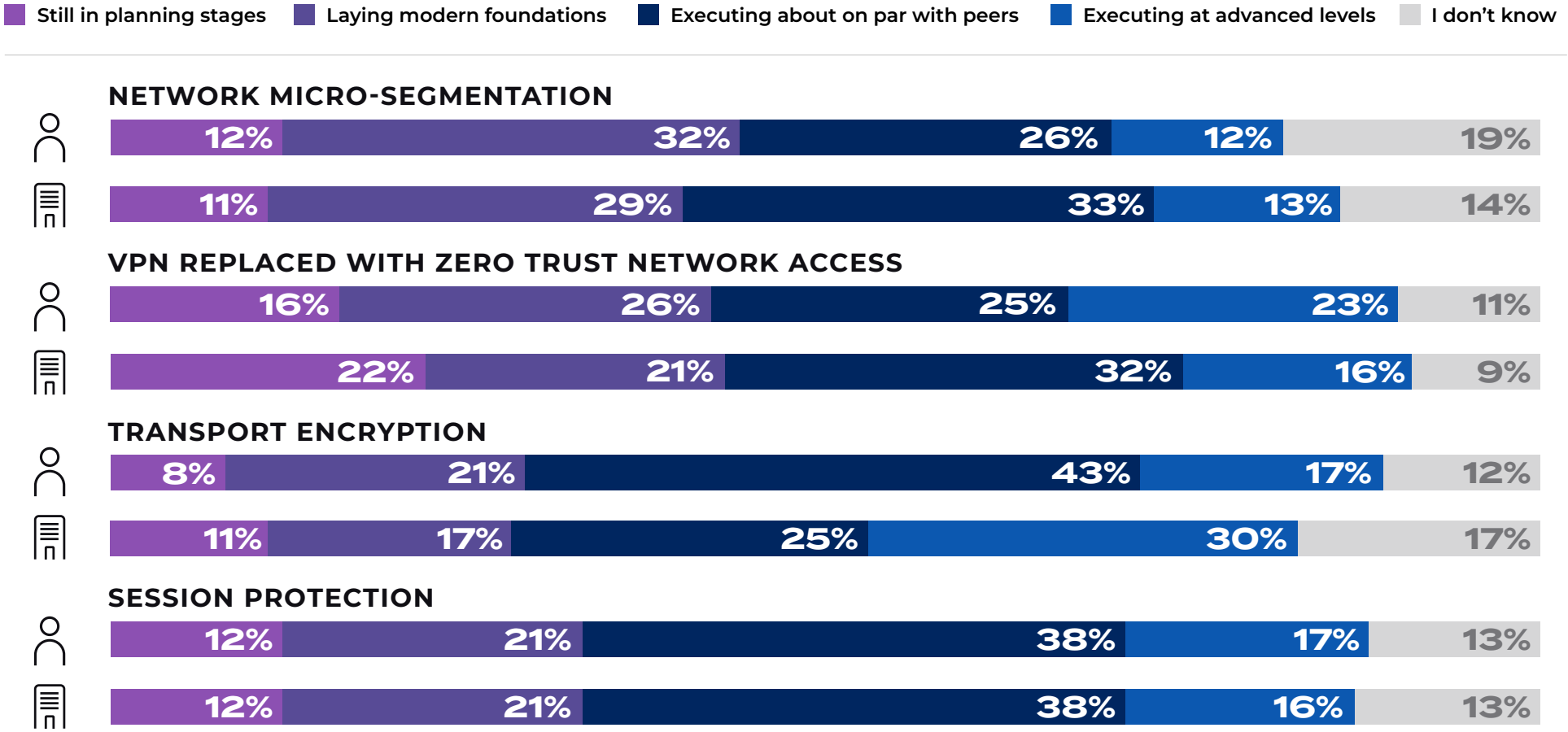
Civilian | Base: 101

Defense & Intelligence | Base: 76

SECURITY CAPABILITIES

Civilian vs. Defense/Intelligence Agencies

How would security experts likely describe where your agency/component is for NETWORK/SESSION TRUST?



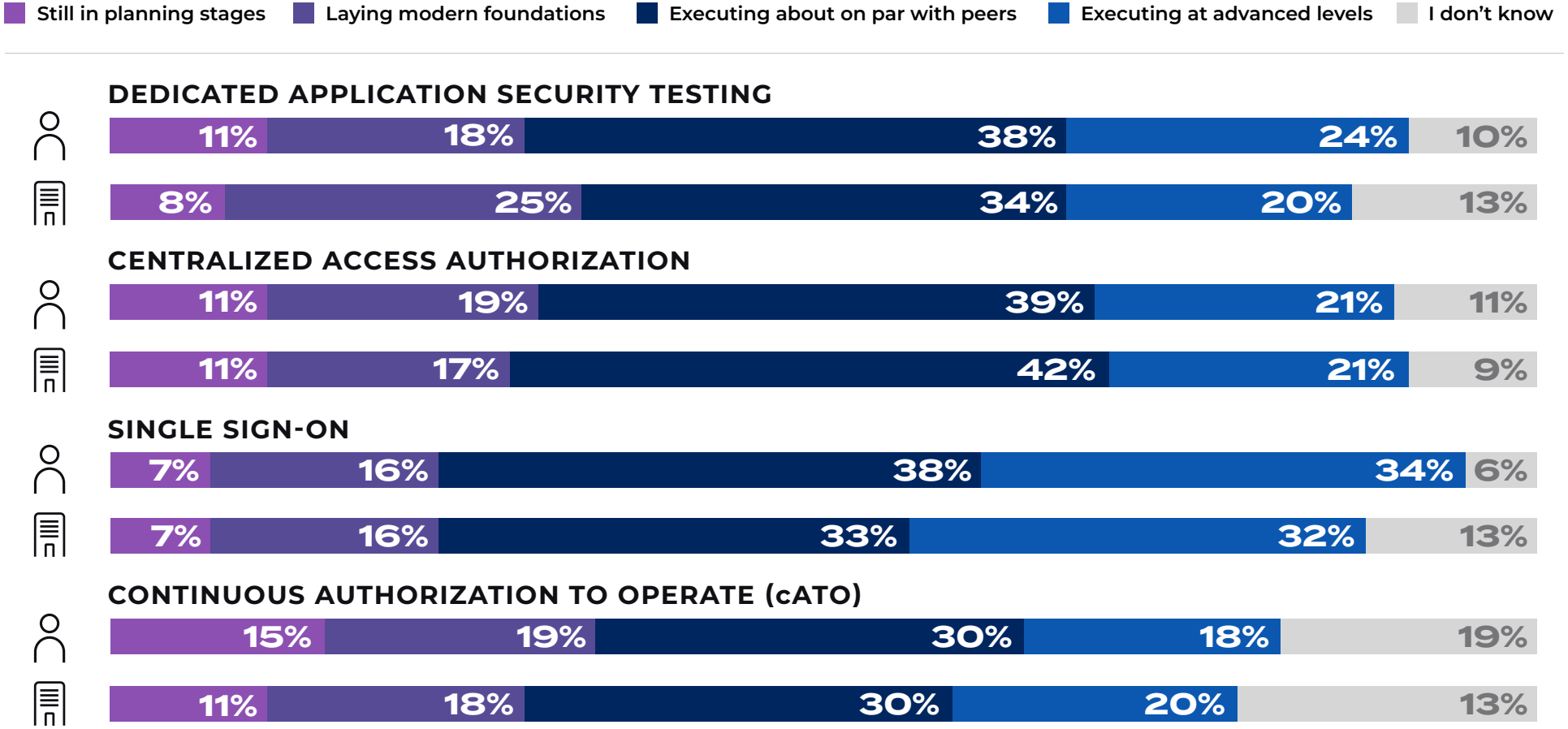
Civilian | Base: 101

Defense & Intelligence | Base: 76

SECURITY CAPABILITIES

Civilian vs. Defense/Intelligence Agencies

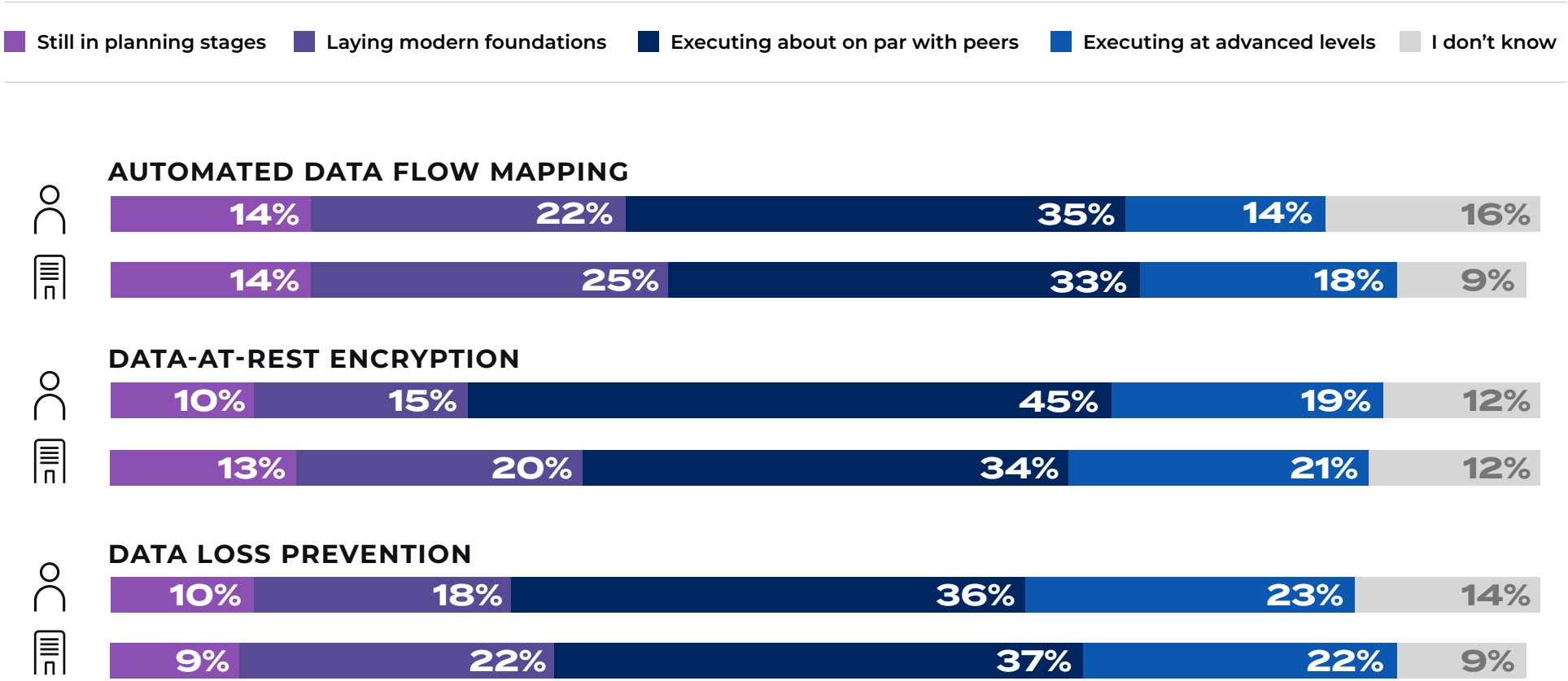
How would security experts likely describe where your agency/component is for APPLICATION TRUST?



SECURITY CAPABILITIES

Civilian vs. Defense/Intelligence Agencies

How would security experts likely describe where your agency/component is for DATA TRUST?



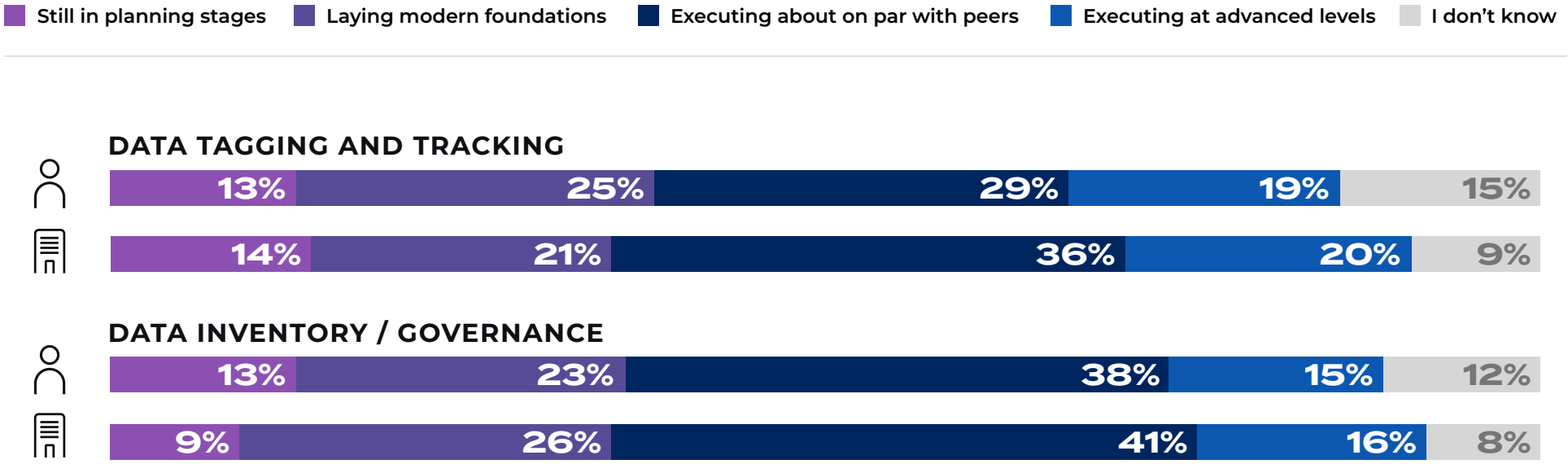
Civilian | Base: 101

Defense & Intelligence | Base: 76

SECURITY CAPABILITIES

Civilian vs. Defense/Intelligence Agencies

How would security experts likely describe where your agency/component is for DATA TRUST?



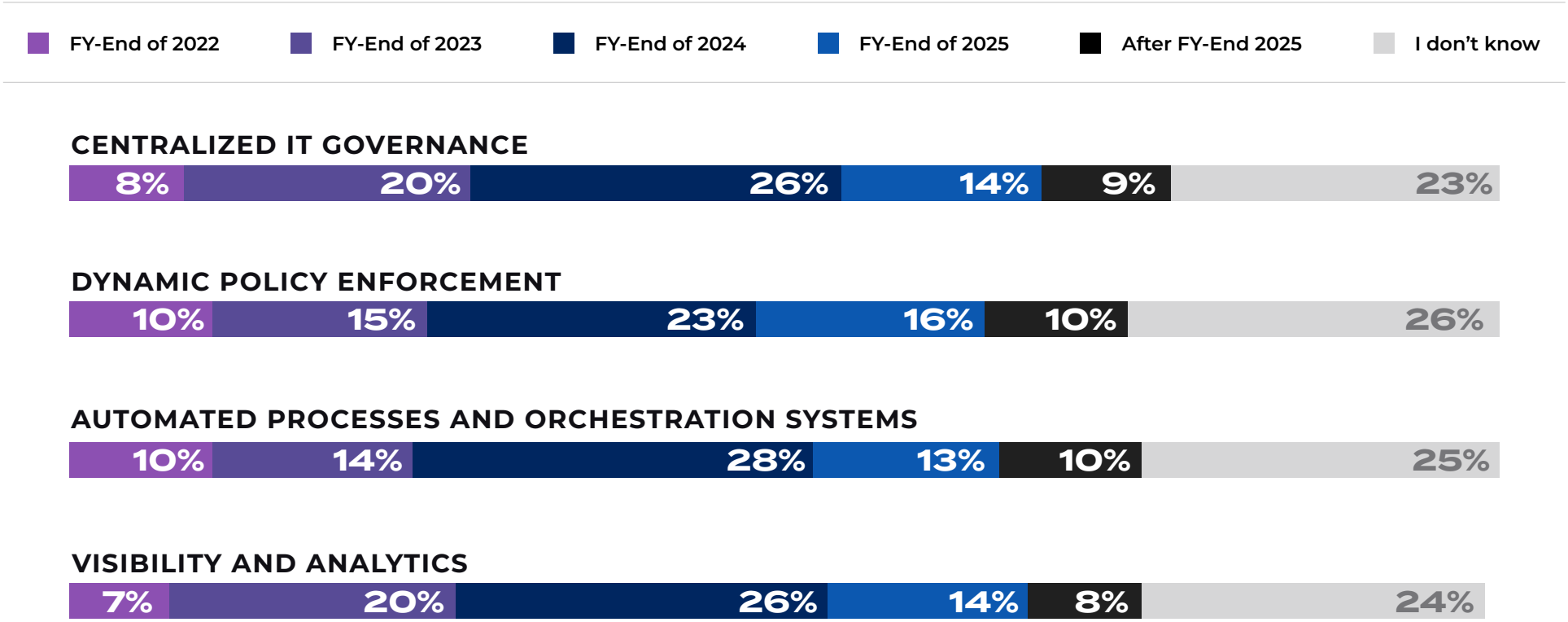
Civilian | Base: 101

Defense & Intelligence | Base: 76

TIMELINE FOR INTEGRATED ENTERPRISE-WIDE SYSTEMS

All respondents

When does your agency/component envision having the following integrated enterprise-wide systems in place to manage trust across all five pillars of zero trust?



TECHNICAL CHALLENGES

All respondents

What are the most significant technical challenges your agency/component currently faces to establish a zero-trust environment?

(Select up to 5)

1. **44% // Interdependency of existing technology**
2. **43% // Conflicting IT priorities**
3. **42% // Complexity of IT environment**
4. **40% // Managing the growth of data**
5. **33% // Advancing zero-trust goals in one pillar, without breaking things in another**
6. **32% // Limited capabilities to view/analyze security issues across all five zero trust pillars**
7. **32% // Proliferation of devices / applications accessing our networks**

DIFFERING VIEWPOINTS:

Among civilian agency respondents, **48%** said the "complexity of IT environment" was the most significant technical challenge compared to **43%** of defense/ intelligence who indicated "conflicting IT priorities."

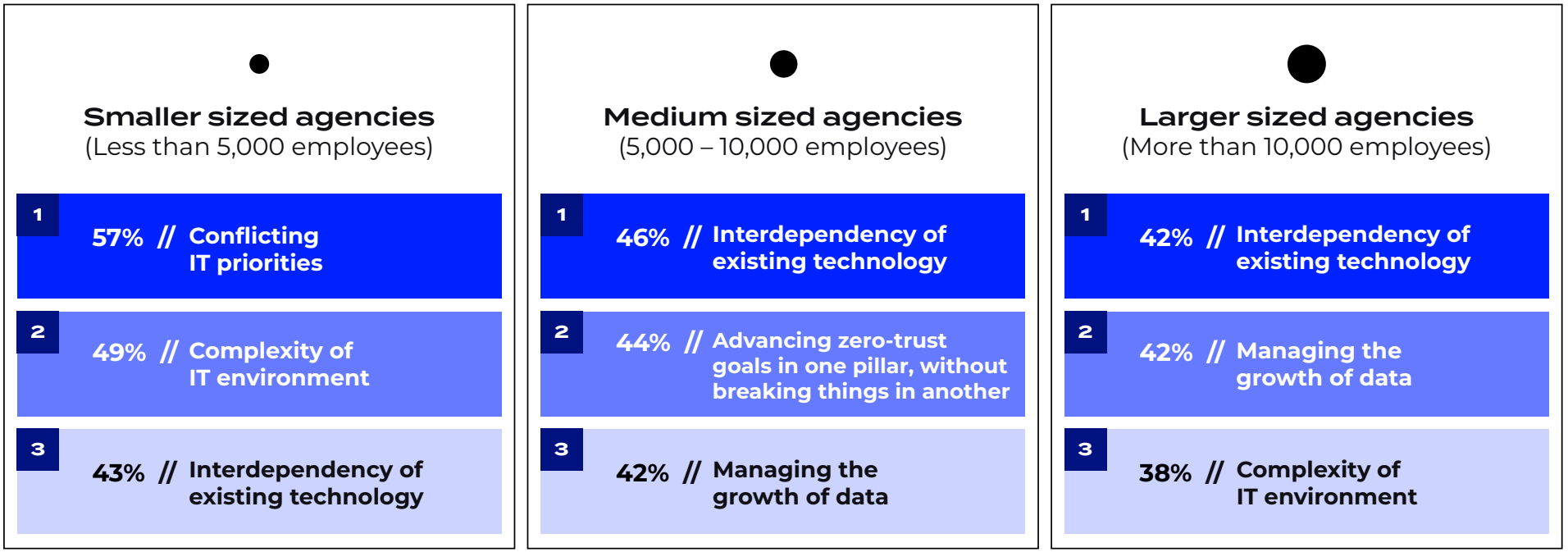
Base: 177

I don't know 12% | Other 5%

TECHNICAL CHALLENGES

Agency size comparison

What are the most significant technical challenges your agency/component currently faces to establish a zero-trust environment?



Base: 47

Base: 52

Base: 78

OPERATIONAL CHALLENGES

All respondents

What are the most significant operational challenges your agency/component currently faces to establish a zero-trust environment?

(Select up to 5)

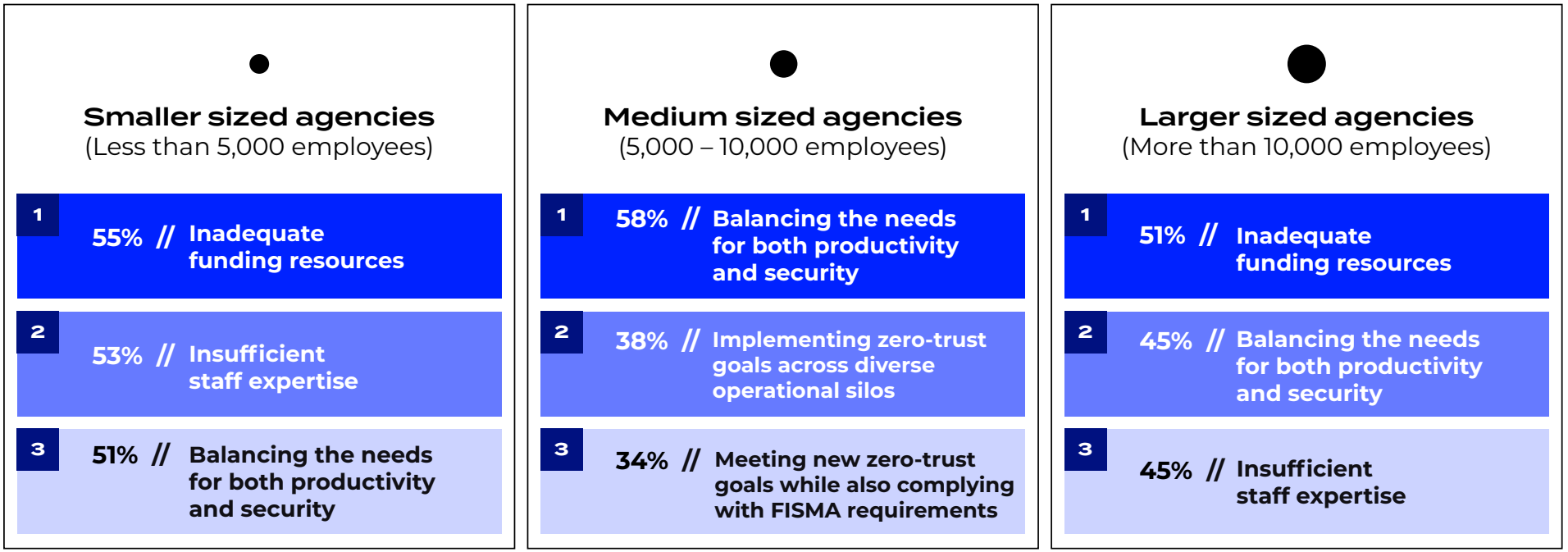
1. **50% // Balancing the needs for both productivity and security**
2. **49% // Inadequate funding resources**
3. **46% // Insufficient staff expertise**
4. **38% // Implementing zero-trust goals across diverse operational silos**
5. **34% // Meeting new zero-trust goals while also complying with FISMA requirements**
6. **26% // Fluidity of users and roles**
7. **21% // Lack of leadership support**
8. **18% // Knowing where to start**

Base: 177
I don't know 8% | Other 3%

OPERATIONAL CHALLENGES

Agency size comparison

What are the most significant operational challenges your agency/component currently faces to establish a zero-trust environment?



Base: 47

Base: 52

Base: 78

HOW TO ACHIEVE ZERO-TRUST GOALS

All respondents

What would help your agency/component most in achieving the White House's zero-trust goals?

(Select up to 4)

1. **44% // Greater near-term IT funding for zero trust implementation**
2. **38% // Greater opportunities to tap the government's Technology Modernization Fund**
3. **34% // Greater flexibility to acquire managed IT/security services**
4. **33% // Greater leadership support to implement zero trust across business silos**
5. **33% // Greater support for reconciling FISMA compliance with zero trust requirements**
6. **27% // Greater clarity from OMB on tackling non-technical (e.g. personnel) practices**
7. **25% // Aligning FISMA scorecard with zero trust requirements**

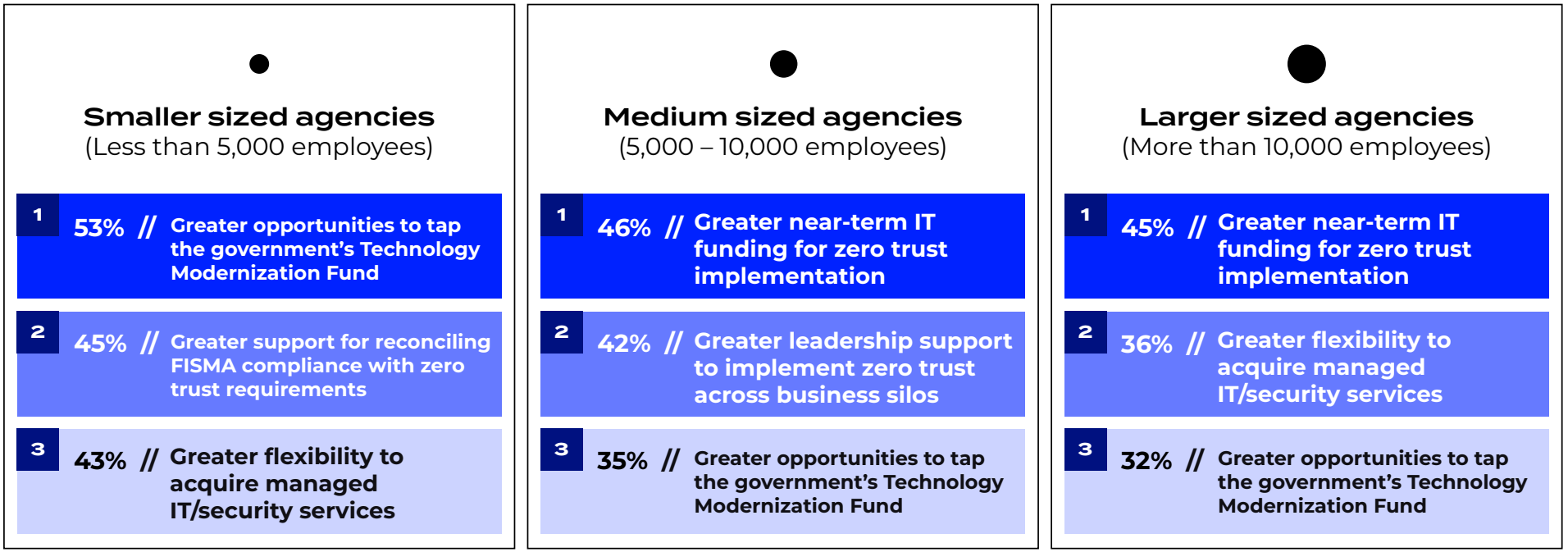
Base: 177

I don't know 15% | Other 3%

HOW TO ACHIEVE ZERO-TRUST GOALS

Agency size comparison

What would help your agency/component most in achieving the White House's zero-trust goals?



Base: 47

Base: 52

Base: 78

MOST INFLUENTIAL ZERO TRUST GUIDANCE

All respondents

Which zero trust guidance has been most influential in directing your agency's/ component's zero trust strategy?

(Select all that apply)

1. **36% // DOD "Zero Trust Reference Architecture"**
2. **34% // White House Executive Order 14028 on "Improving the Nation's Cybersecurity"**
3. **30% // White House OMB Memo M-22-09 on "Moving toward zero trust cybersecurity principles"**
4. **27% // NIST "Zero Trust Architecture" (SP 800-207)**
5. **25% // GSA "Zero Trust Architecture" Buyer's Guide**
6. **24% // CISA "Zero Trust Maturity Model"**
7. **19% // NSA "Embracing a Zero Trust Security Model"**
8. **18% // CISA "Applying Zero Trust Principles to Enterprise Mobility (Draft)"**

DIFFERING VIEWPOINTS:

Among civilian agency respondents, **39%** said the White House EO 14028 was the most influential source of guidance compared to **55%** at defense/intelligence agencies who cited DOD's "Zero Trust Reference Architecture."

Base: 177

Other 6%

CONCLUSIONS

WHERE'S THE MONEY?

The White House Executive Order and OMB's ambitious directives around zero trust provide agencies a clear roadmap — but practically no funding. One in 4 civilian agency leaders polled — and 1 in 5 at defense/intelligence agencies — predict implementing zero trust will consume 10% or more of their annual IT budgets in FY 2023 and 2024; and roughly 2 in 3 respondents believe 4% and more of their IT budgets will need to be redirected to meet OMB's goals.

BETWEEN THE LINES

Roughly half to two-thirds of respondents described various key zero-trust security capabilities as being on par with their peers, or better. But in all likelihood, most capabilities — such as user identity and access controls — are only partially in place or operational. Consequently, agency leaders may be overoptimistic, and have a steeper road ahead of them than they fully recognize.

GETTING TO DYNAMIC ENFORCEMENT

Zero trust requires access to resources provisioned by dynamic policy enforcement at scale. Consequently, federal agencies that have complex IT environments with too much interdependency on existing technology will struggle that much more to lay the foundations needed to achieve OMB's zero trust objectives.

PILLAR BY PILLAR

Identity and access management is central to everything else in zero trust and, fortunately, that's where respondents said their agencies are prioritizing their current security investments. But the other four pillars of zero trust — for securing devices, networks, applications and data, and the tools for automating and orchestrating them — will depend on available IT funds and take years to fully complete.

ACHIEVING ZERO TRUST

Zero trust is the right approach to improving cybersecurity. But without the force of law, and dedicated funding, the promise of zero trust will likely take far longer to achieve than federal officials believe.

FEDSCOOP

FedScoop is the leading tech media brand in the federal government market. With more than 4.3 million monthly unique engagements and 202,000 daily newsletter subscribers, FedScoop gathers top leaders from the White House, federal agencies, academia and the tech industry to discuss ways technology can improve government and identify ways to achieve common goals. With our website, newsletter and events, we've become the community's go-to platform for education and collaboration.

CONTACT

Wyatt Kash

Senior Vice President Content Strategy
Scoop News Group
Washington, D.C. 202.887.8001
wyatt.kash@scoopnewsgroup.com