IT INSIGHTS REPORT

SECURING THE EDGE

How federal agencies are moving forward to meet the White House Executive Order on Cybersecurity

This report surveyed federal agency leaders and IT decision-makers to explore where they are in their adoption of new federal mandates on cybersecurity and uncover trends among agencies to strengthen security at edge of the network.

PRESENTED BY CYBERSCOOP | FEDSCOOP

UNDERWRITTEN BY Lookout

EXECUTIVE SUMMARY

With the release of the White House's Cybersecurity Executive Order (EO), federal agencies are tackling a wide range of cybersecurity mandates, which now include timelines to adopt zero-trust security architecture.

CyberScoop and FedScoop surveyed federal agency leaders and IT decision-makers to understand the challenges agencies continue to face in their efforts to strengthen security at edge of the network.

This survey of 162 prequalified program leaders and IT decision makers at federal civilian, defense and intelligence agencies, took a fresh look at how organizations are evolving their cybersecurity plans.

SPECIFICALLY, THE STUDY:

- Explored the impact of the executive order in getting agency leaders to commit resources toward critical cybersecurity projects.
- Assessed perceptions on the maturity of agencies' zero-trust strategies.
- Examined capabilities agencies are equipped with to manage security.
- Gauged executives' views on moving toward Secure Access Service Edge (SASE) security solutions over the next three years.

EXECUTIVE SUMMARY

While the findings reinforced that agencies are evolving their cybersecurity plans to abide by the EO on cybersecurity, they also revealed that agency executives, contractors and system integrators at times differ in their views about priorities, challenges, progress and agency maturity in managing security.

KEY FINDINGS:

Progress on strategy building – The findings show contractors and integrators believe more work needs to be done to complete EO cyber strategies than do agency leaders:

- 38% of **federal employees** believe "all of the strategies" required to date have been developed and 35% believe "roughly 75% or more" of the strategies have been developed.
- 25% of **contractors and system integrators** believe "all of the strategies" have been developed while 54% estimate roughly 75% or more of them have been developed.

Maturity in managing a zero-trust security environment – Respondents indicated that their agency had relatively high degrees of maturity in managing five key components of zero trust:

- More than 7 in 10 respondents said their ability to manage data, application workload, network/applications and devices were either advanced or optimally configured; and 6 in 10 rated identity and access comparably mature.

Capabilities to manage security – When it comes to how well-equipped agencies are to manage security:

- 2 in 3 respondents said their agency can continuously monitor risk on traditional endpoints and roughly half can do so on mobile devices.
- Only 1 in 3 federal employees – and fewer contractors and system integrators – said agencies are able to secure data regardless of where it goes.

EXECUTIVE SUMMARY

Cybersecurity priorities – When asked about the biggest priorities driving efforts to achieve zero trust beyond the EO, the findings show:

- 62% of **federal employees** believe protecting data is the most important followed by preventing breaches (57%) and securing endpoints (56%).
- 62% of **contractors and system integrators** ranked securing endpoints as the biggest priority followed by protecting data (52%), reducing new risks from IoT and preventing breaches both at 48%.

When comparing agencies, 67% **federal civilian** respondents ranked protecting data as highest while 50% **defense** and 67% **intelligence** agency respondents selected securing endpoints as the highest priority.

Findings show modernizing systems as the lowest priority when comparing agencies as well as employer type.

Challenges in establishing zero trust – The findings show differences in what is seen as significant challenges:

- 57% of **federal employees** believe the complexity of environment and conflicting IT priorities (54%) are the most significant challenges.
- 58% of **contractors and system integrators** believe conflicting IT priorities and proliferation of devices accessing networks (48%) are most significant.
- 63% of **defense** agency respondents believe conflicting IT priorities is most challenging followed by complexity of environments (53%).
- 53% of **civilian agency** respondents also ranked IT priorities and limited budget resources as most significant challenges.
- 58% of **intelligence** agency respondents ranked interdependency of existing technology as highest followed by conflicting IT priorities.

WHO WE SURVEYED

CyberScoop and FedScoop conducted an online survey of 162 prequalified respondents. The survey was conducted online in December 2021.

RESPONDENT BY AGENCY

Federal civilian	52%
Intelligence	28%
Defense	20%

RESPONDENT BY EMPLOYER

Federal agency	60%
Government contractor	20%
System integrator	20%

RESPONDENT BY AGENCY SIZE

5,000 – 10,000 employees	50%
Less than 5,000 employees	33%
More than 10,000 employees	17%

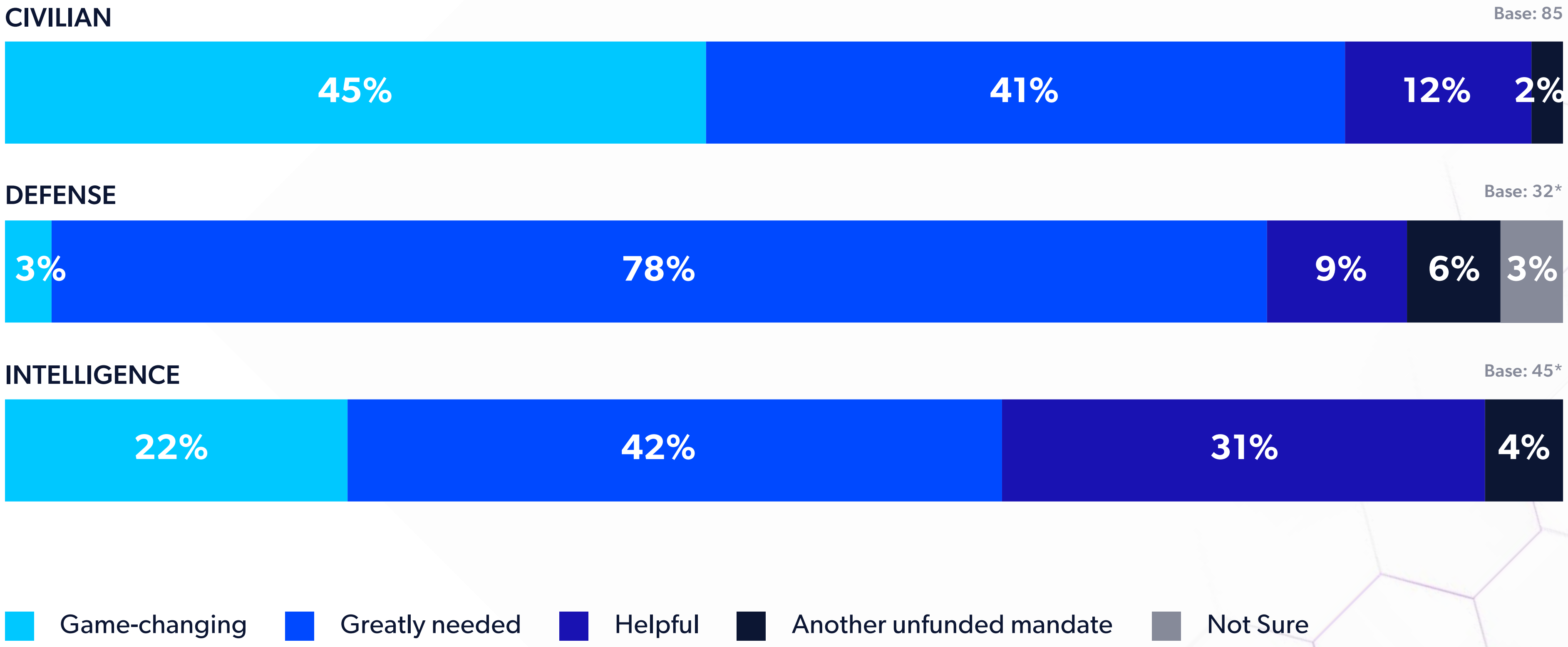
RESPONDENT BREAKOUT BY JOB TITLE

IT management/staff	45%
C-suite/senior business/program leader	19%
IT security management/staff	15%
CIO, CTO CISO	10%
IT influencer	4%
Procurement official/staff	3%
Other *(e.g. IT specialist, systems specialist, supervisor)*	2%

IMPACT OF CYBERSECURITY INITIATIVES

AGENCY COMPARISON

How would you describe the impact of the White House Cybersecurity Executive Order in getting agency leaders to commit resources toward critical cybersecurity projects?



* Caution: Margin of error increases with a small base.

PROGRESS OF BUILDING STRATEGY

ALL RESPONDENTS

How much progress has your agency made to date with building strategies around the EO?

4%

Still developing the required strategies

5%

Roughly 25% of the strategies required to date have been developed

15%

Roughly 50% of the strategies required to date have been developed

43%

Roughly 75% of the strategies required to date have been developed

33%

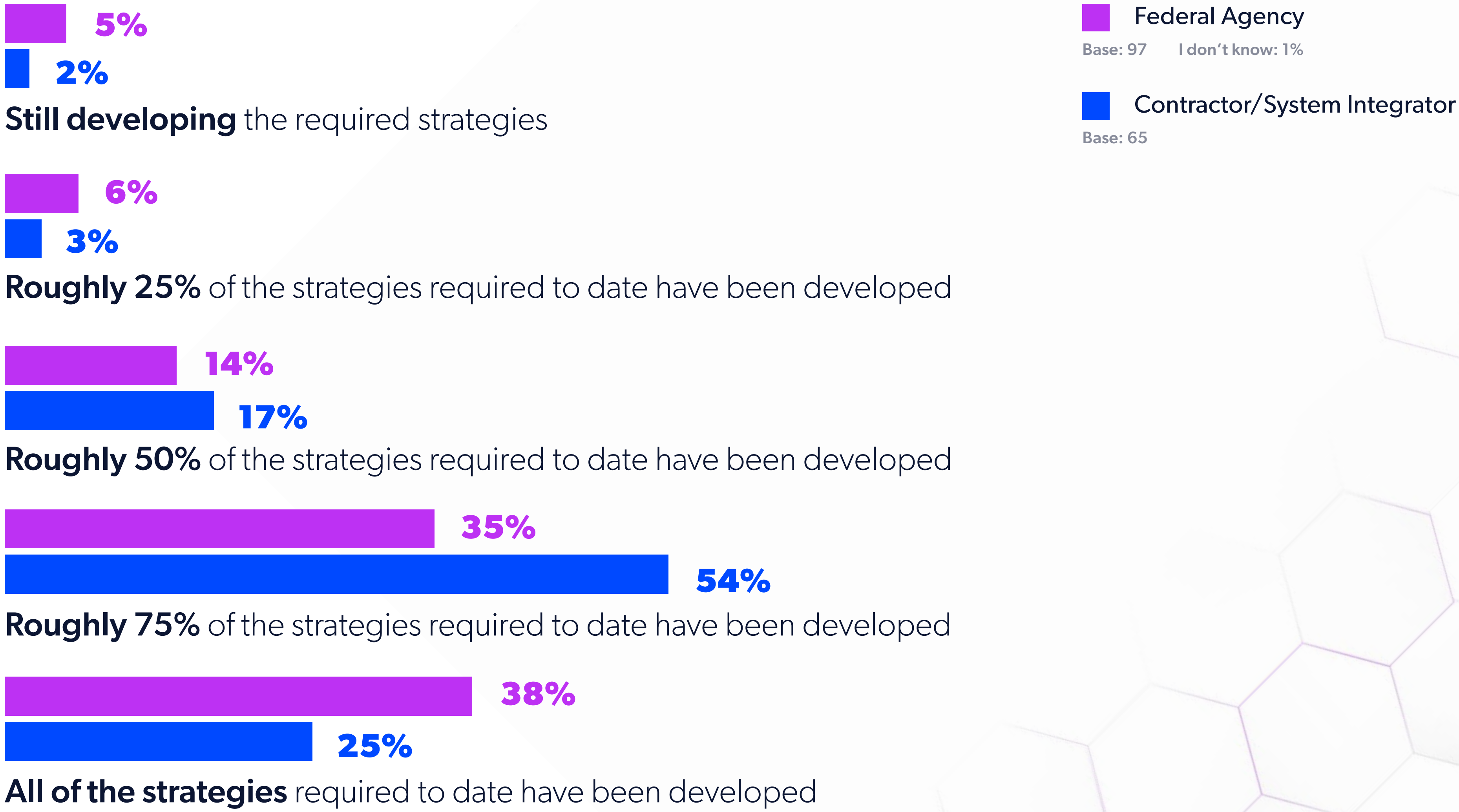
All of the strategies required to date have been developed

Base: 162   I don't know: 1%

PROGRESS OF BUILDING STRATEGY

FEDERAL AGENCY VS CONTRACTOR, SYSTEM INTEGRATOR

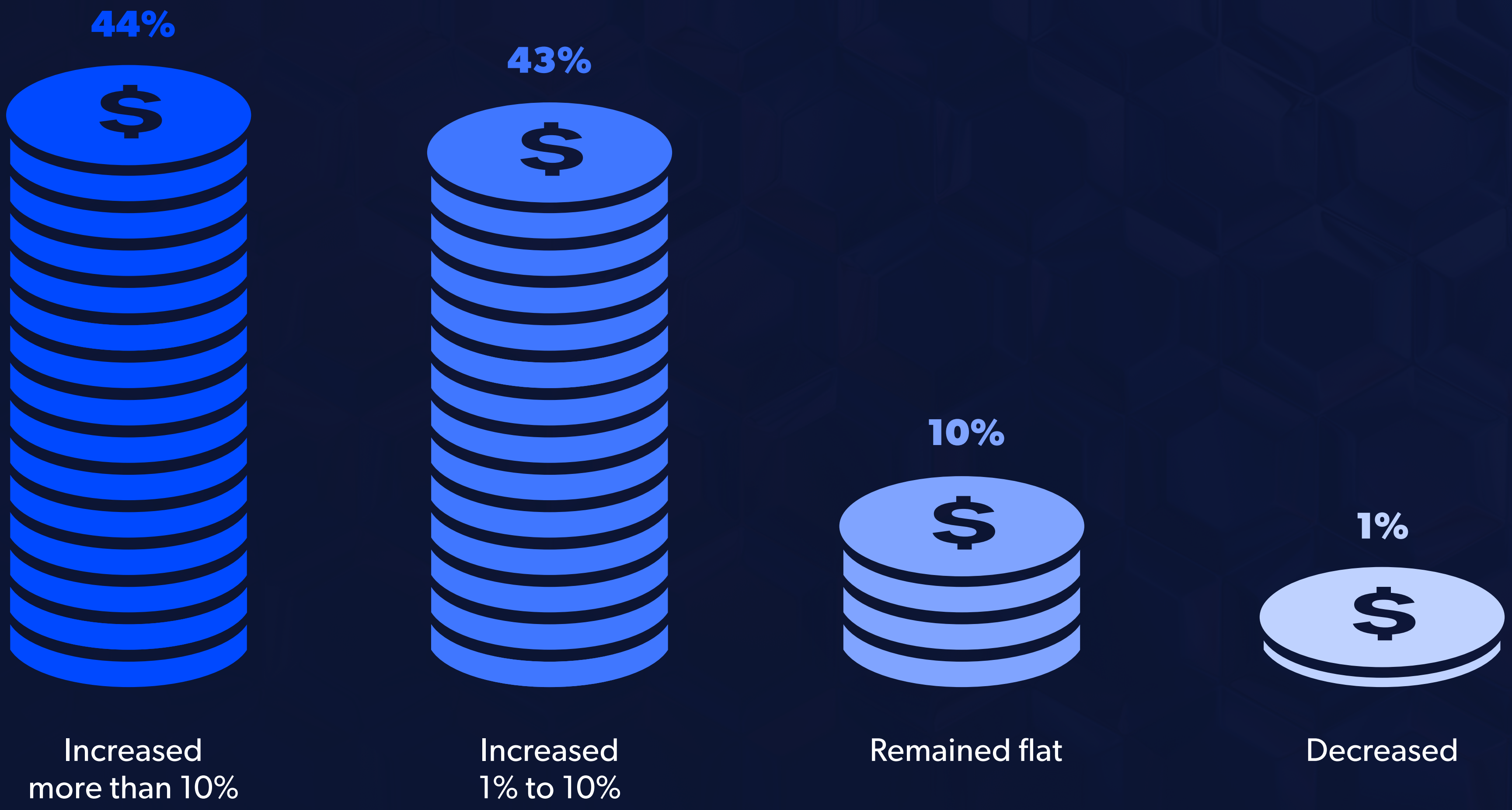
How much progress has your agency made to date with building strategies around the EO?



SECURITY BUDGET IN 2022

ALL RESPONDENTS

How have your IT Security Fiscal Year 2022 budgets changed to meet the White House Cybersecurity Executive Order requirements?



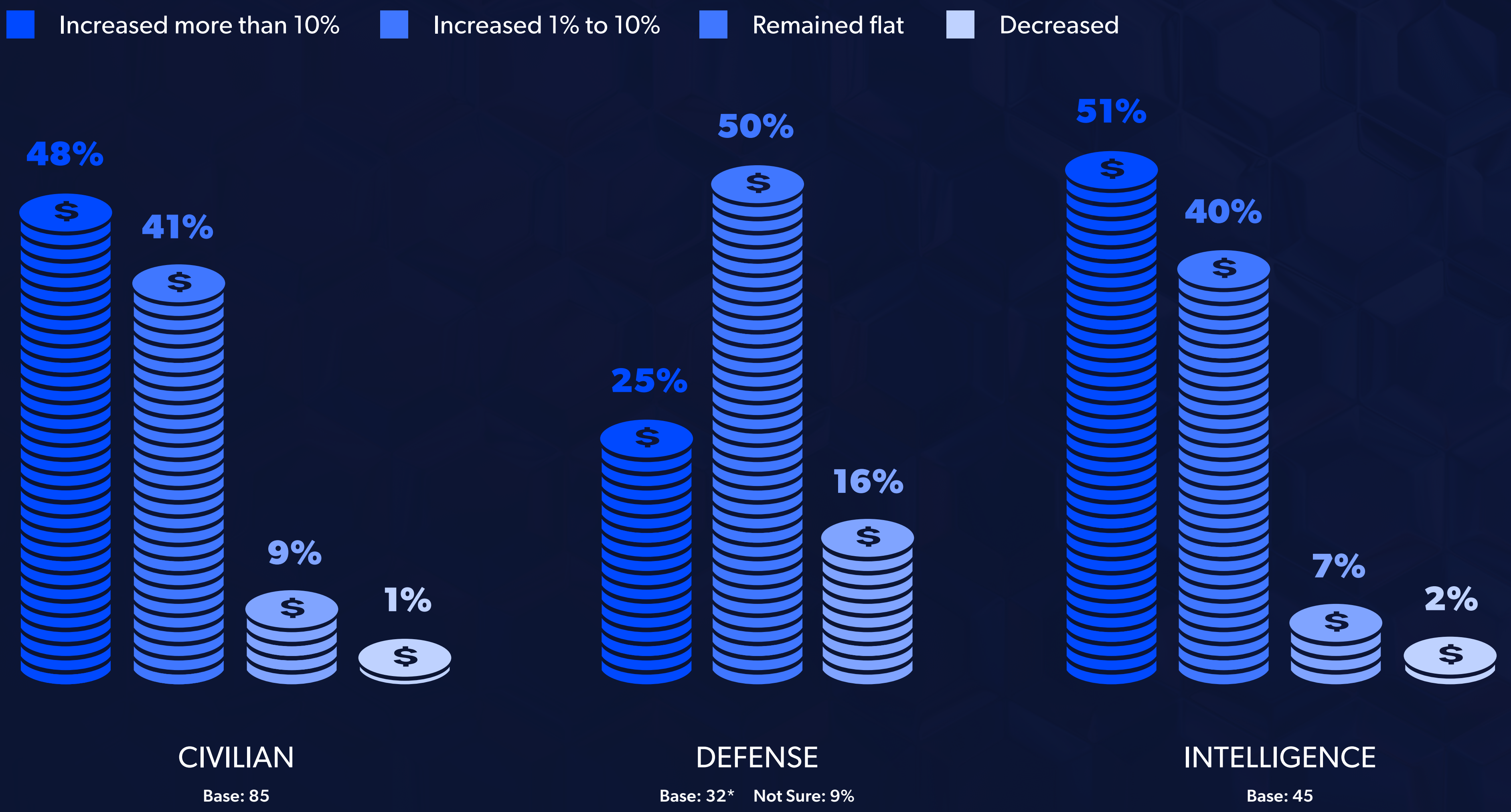
Base: 162 Not Sure: 2%

CYBERSCOOP | FEDSCOOP

SECURITY BUDGET IN 2022

AGENCY COMPARISON

How have your IT Security Fiscal Year 2022 budgets changed to meet the White House Cybersecurity Executive Order requirements?



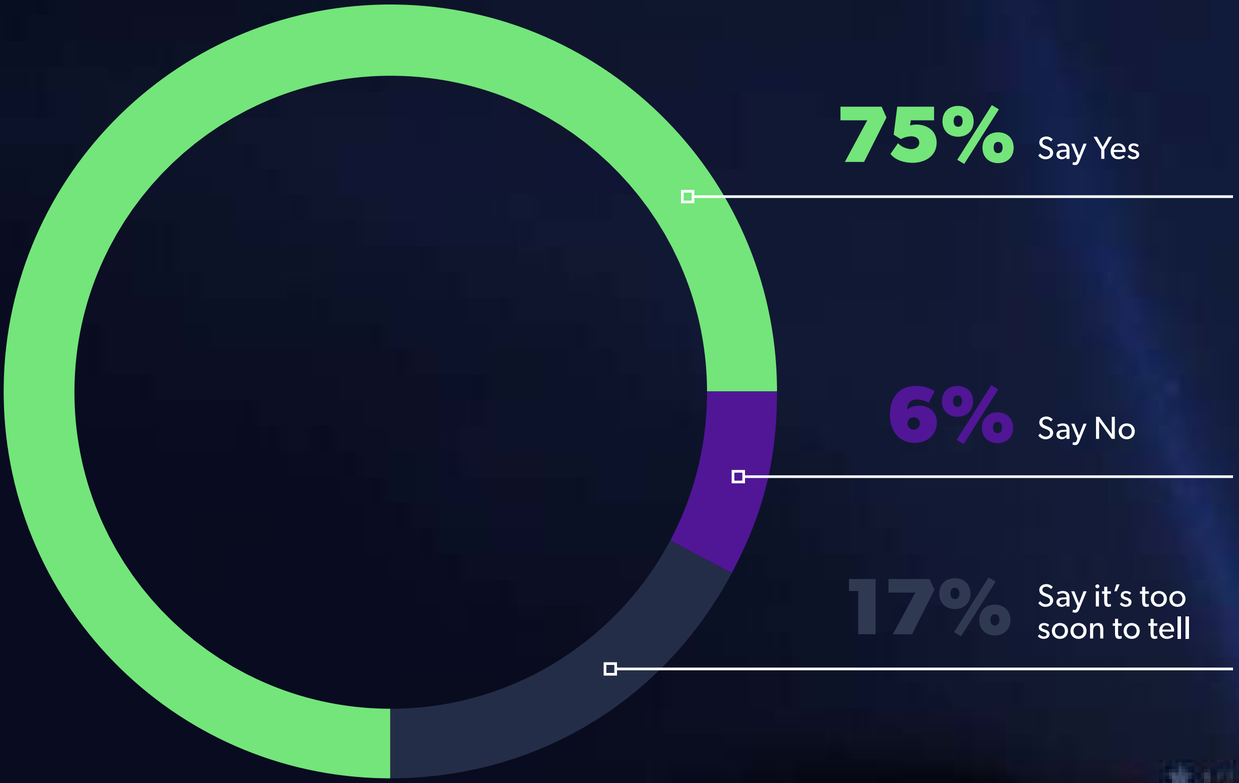
* Caution: Margin of error increases with a small base.

CYBERSCOOP | FEDSCOOP

REMOVING BARRIERS TO SHARE THREAT INFORMATION

ALL RESPONDENTS

Have efforts by the White House and OMB to revise federal contract language to “remove barriers to sharing threat information” been adequate to help meet the Executive Order’s cybersecurity objectives?

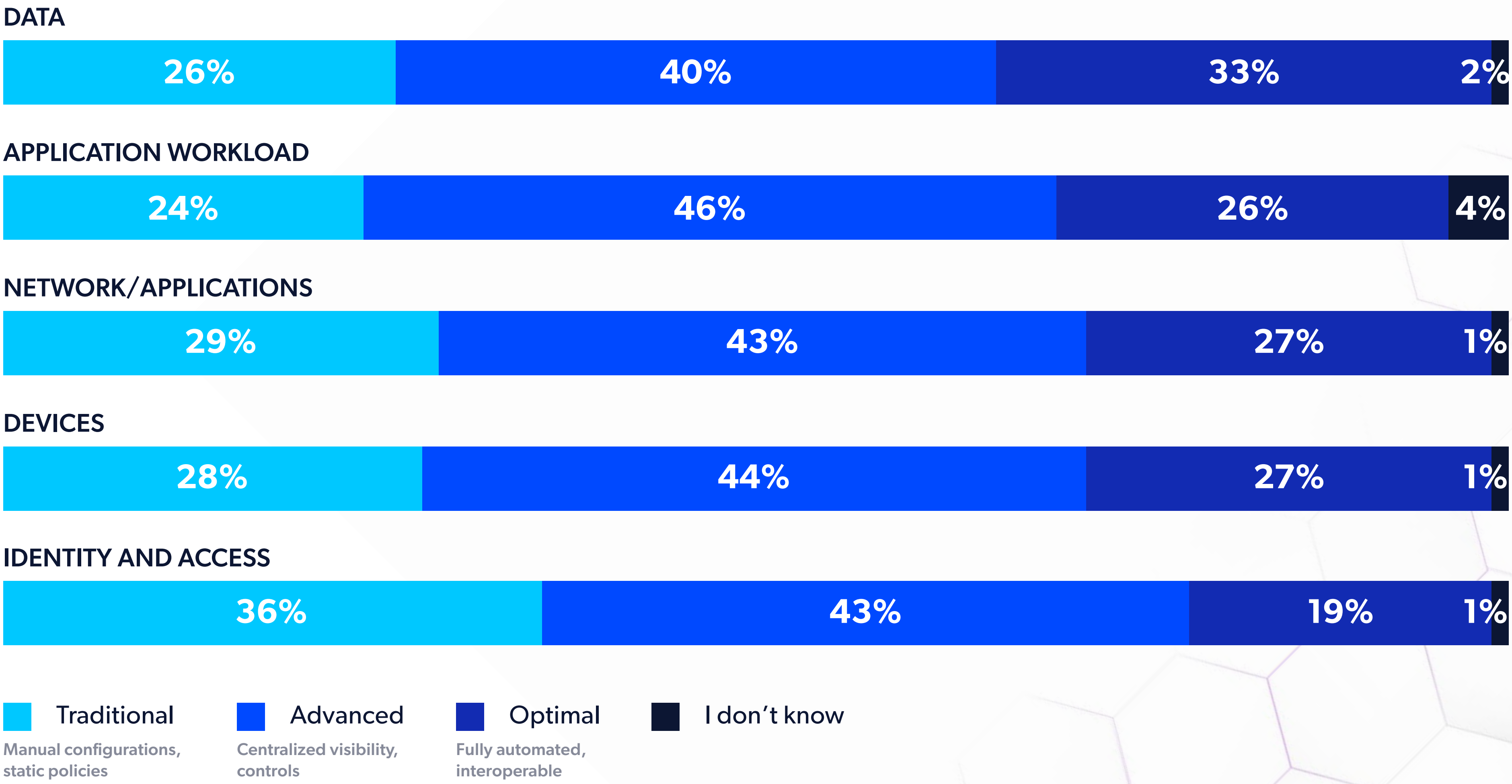


Base: 162   I don’t know: 2%

ZERO-TRUST MATURITY

ALL RESPONDENTS

When it comes to establishing a zero-trust environment, how would you rate your agency's maturity in the following areas?

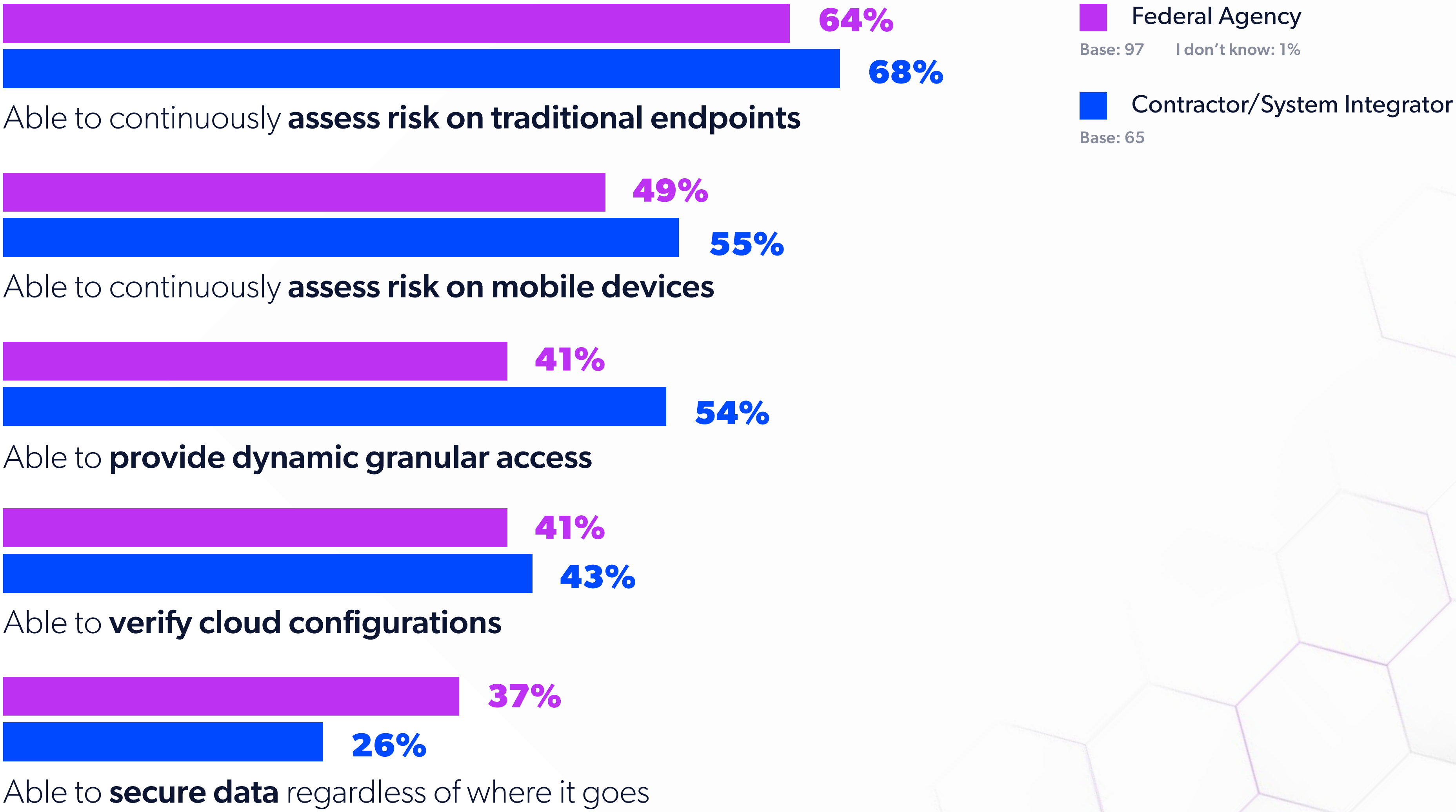


Base: 162

SECURITY MANAGEMENT CAPABILITIES

FEDERAL AGENCY VS CONTRACTOR, SYSTEM INTEGRATOR

Which capabilities are your agency most well equipped with today to manage security? (Select up to 3)

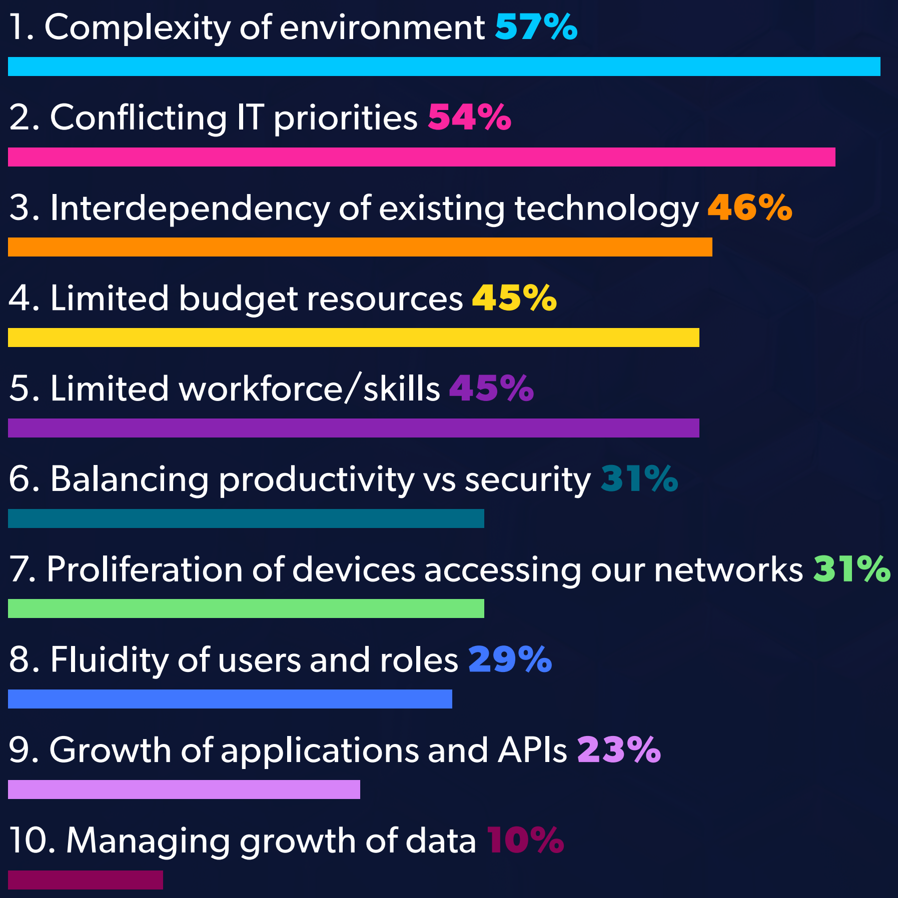


CHALLENGES

FEDERAL AGENCY VS CONTRACTOR, SYSTEM INTEGRATOR

What are the most significant challenges to establishing a zero-trust environment? ? (Select up to 5)

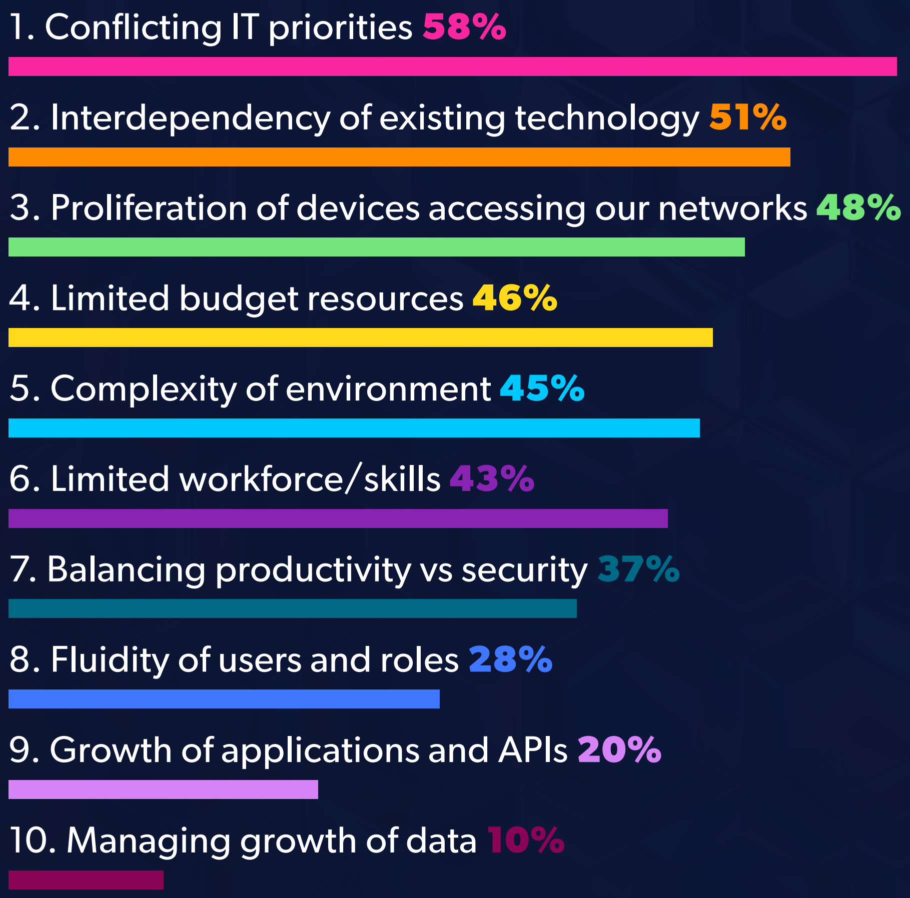
FEDERAL AGENCY



1. Complexity of environment **57%**
2. Conflicting IT priorities **54%**
3. Interdependency of existing technology **46%**
4. Limited budget resources **45%**
5. Limited workforce/skills **45%**
6. Balancing productivity vs security **31%**
7. Proliferation of devices accessing our networks **31%**
8. Fluidity of users and roles **29%**
9. Growth of applications and APIs **23%**
10. Managing growth of data **10%**

Base: 97

CONTRACTOR, SYSTEM INTEGRATOR

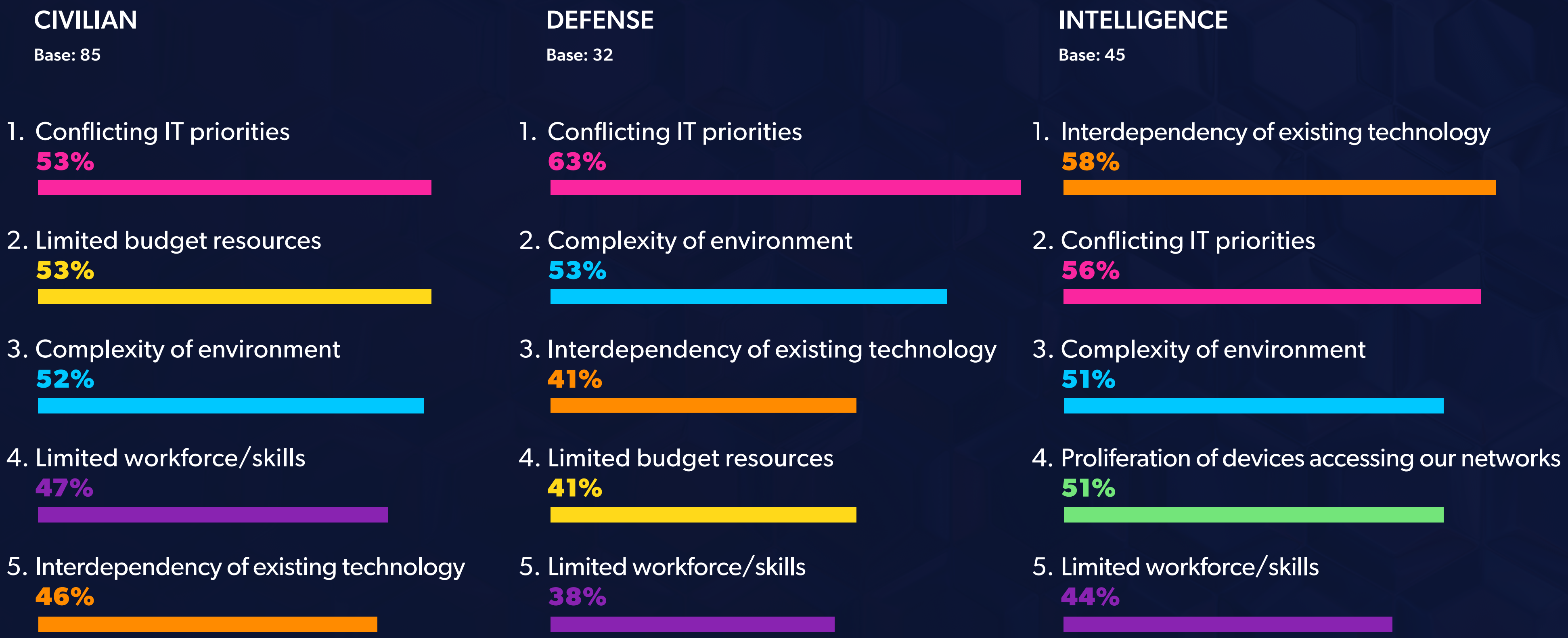


1. Conflicting IT priorities **58%**
2. Interdependency of existing technology **51%**
3. Proliferation of devices accessing our networks **48%**
4. Limited budget resources **46%**
5. Complexity of environment **45%**
6. Limited workforce/skills **43%**
7. Balancing productivity vs security **37%**
8. Fluidity of users and roles **28%**
9. Growth of applications and APIs **20%**
10. Managing growth of data **10%**

Base: 65

CHALLENGES
AGENCY COMPARISON

What are the most significant challenges to establishing a zero-trust environment? (Select up to 5)



CIVILIAN

Base: 85

1. Conflicting IT priorities
   53%
2. Limited budget resources
   53%
3. Complexity of environment
   52%
4. Limited workforce/skills
   47%
5. Interdependency of existing technology
   46%

DEFENSE

Base: 32

1. Conflicting IT priorities
   63%
2. Complexity of environment
   53%
3. Interdependency of existing technology
   41%
4. Limited budget resources
   41%
5. Limited workforce/skills
   38%

INTELLIGENCE

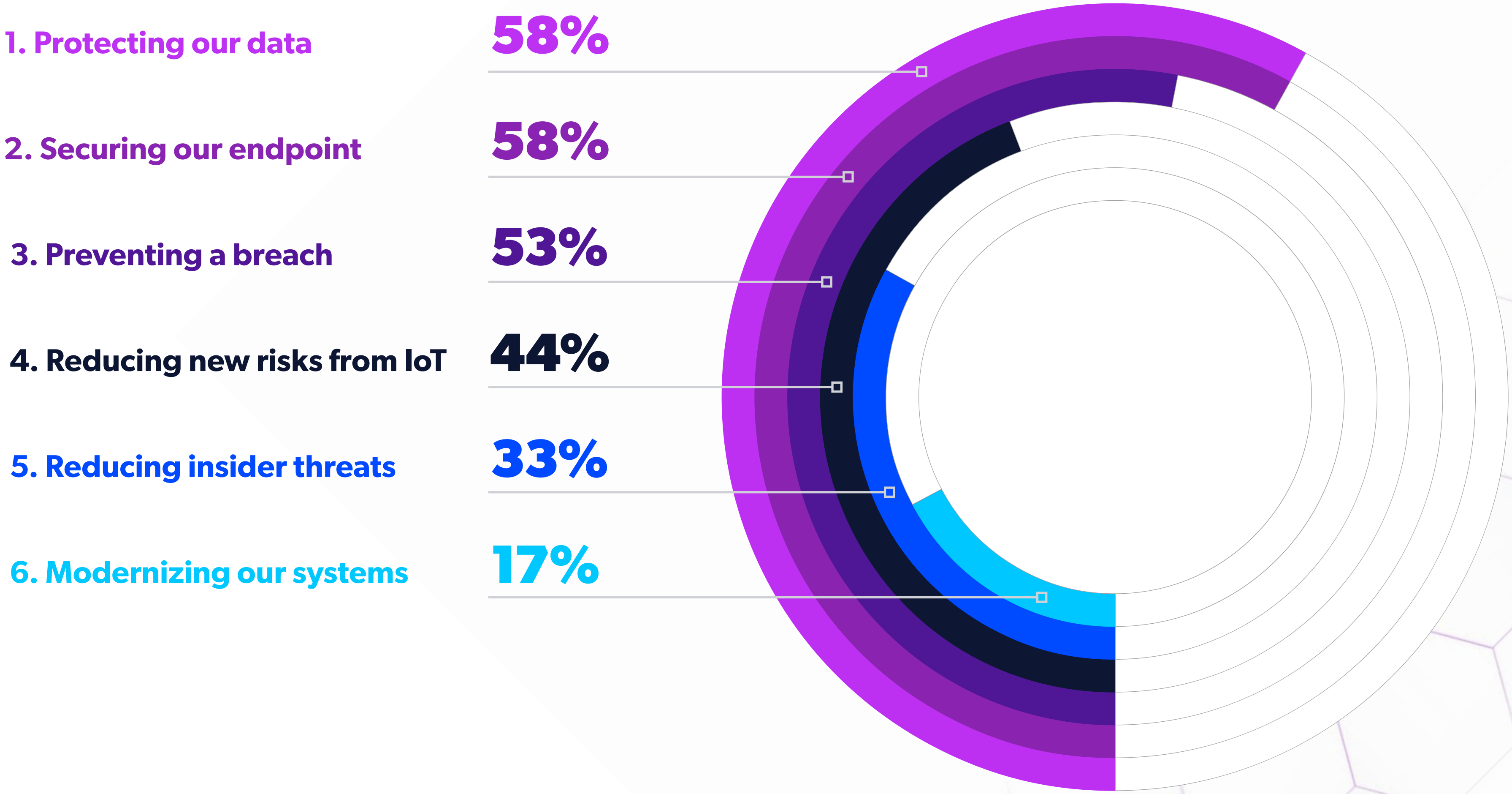
Base: 45

1. Interdependency of existing technology
   58%
2. Conflicting IT priorities
   56%
3. Complexity of environment
   51%
4. Proliferation of devices accessing our networks
   51%
5. Limited workforce/skills
   44%

PRIORITIES DRIVING ZERO TRUST

ALL RESPONDENTS

What are the biggest priorities driving your organization's efforts to achieve zero trust beyond the White House Executive Order itself? (Select up to 3)



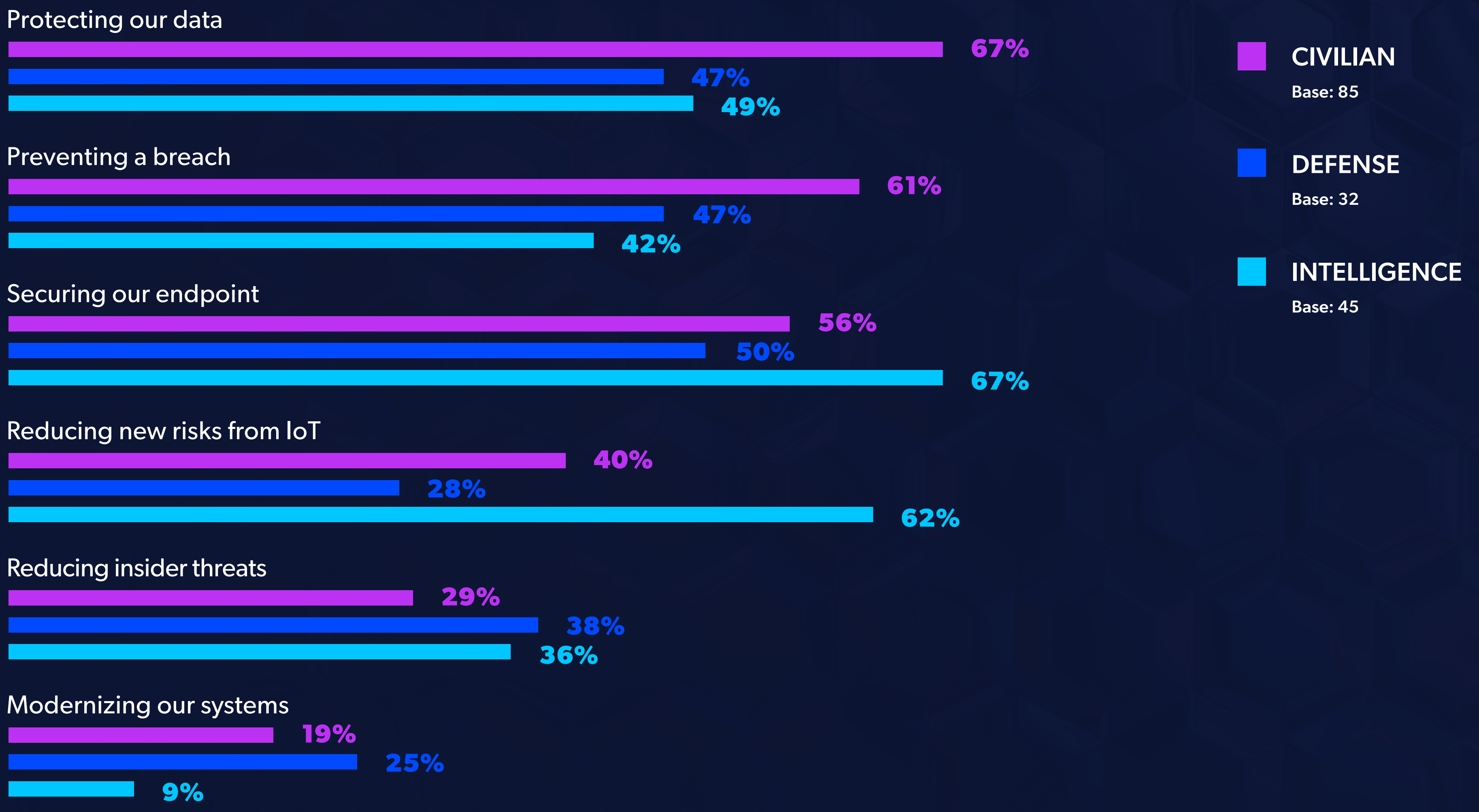
1. Protecting our data	58%
2. Securing our endpoint	58%
3. Preventing a breach	53%
4. Reducing new risks from IoT	44%
5. Reducing insider threats	33%
6. Modernizing our systems	17%

Base: 162

PRIORITIES DRIVING ZERO TRUST

AGENCY COMPARISON

What are the biggest priorities driving your organization's efforts to achieve zero trust beyond the White House Executive Order itself? (Select up to 3)

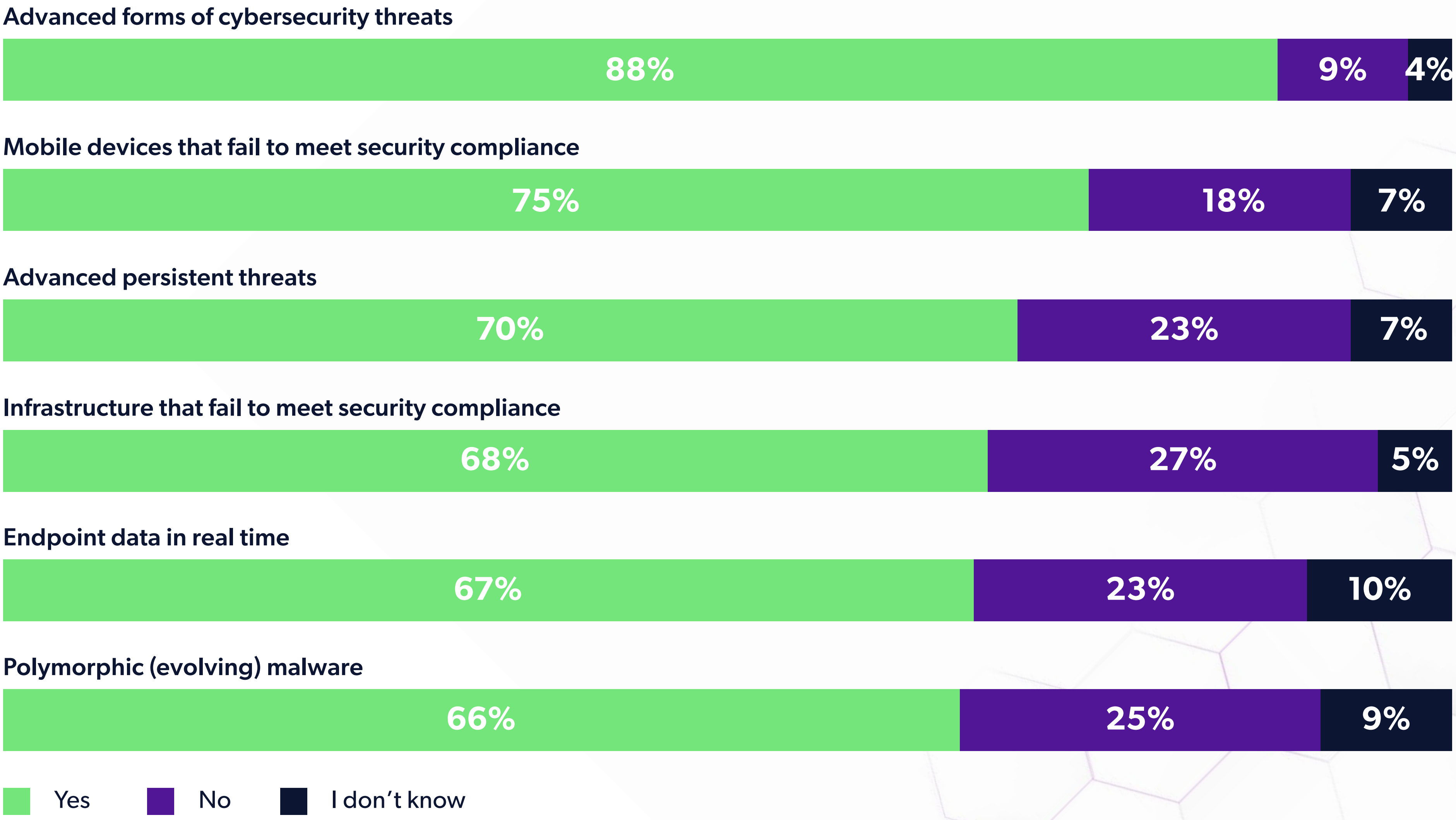


CYBERSCOOP | FEDSCOOP

IMPLEMENTING ENDPOINT DETECTION AND RESPONSE

ALL RESPONDENTS

When it comes to implementing Endpoint Detection and Response (EDR), does your agency currently have the ability to perform the following EDR activities with relative consistency?



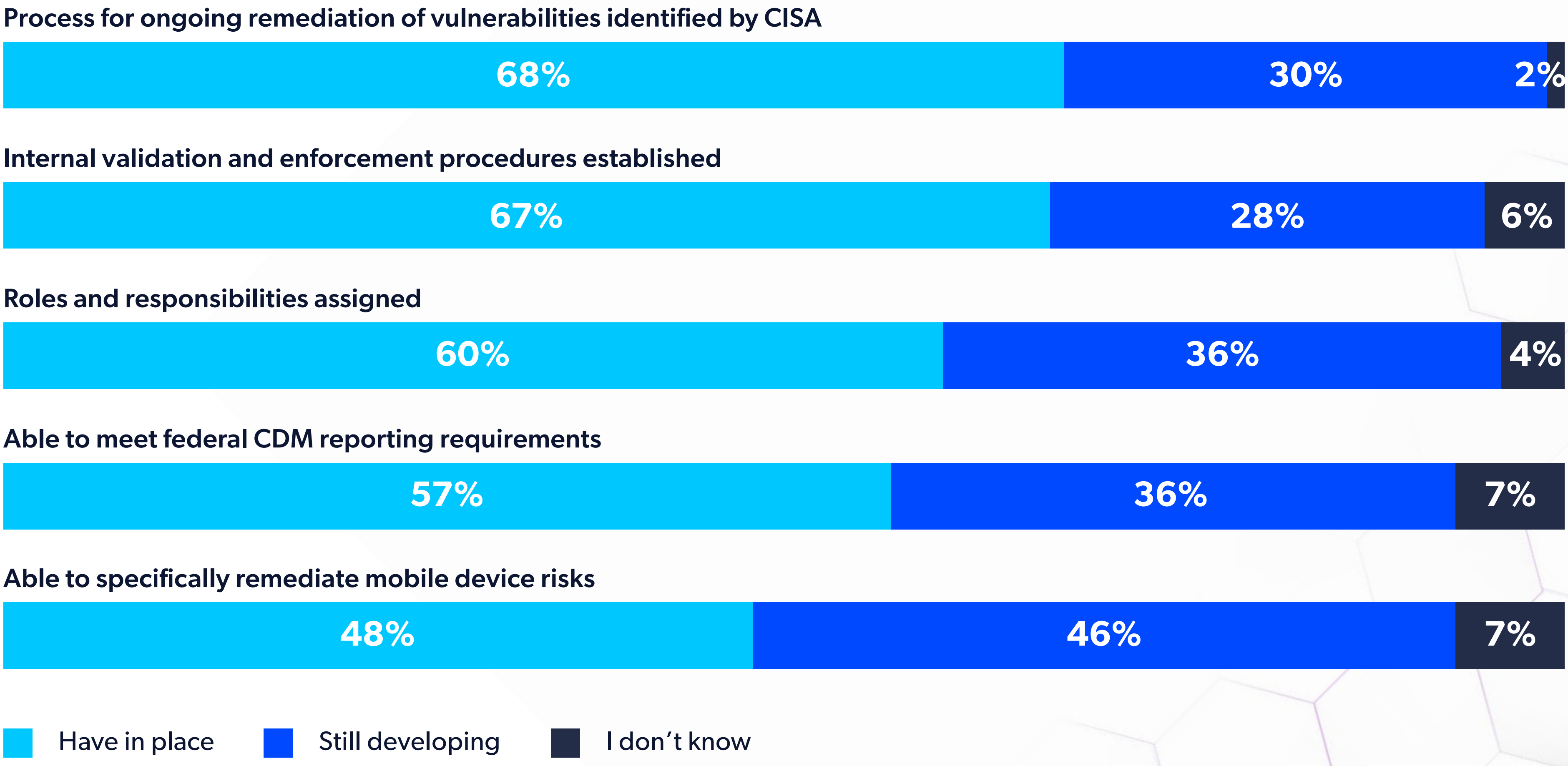
Base: 162

CYBERSCOOP | FEDSCOOP

REDUCING VULNERABILITIES

ALL RESPONDENTS

How prepared is your organization to "significantly reduce known exploited vulnerabilities" as directed by DHS/CISA in "Binding Directive 22-01?"



Base: 162

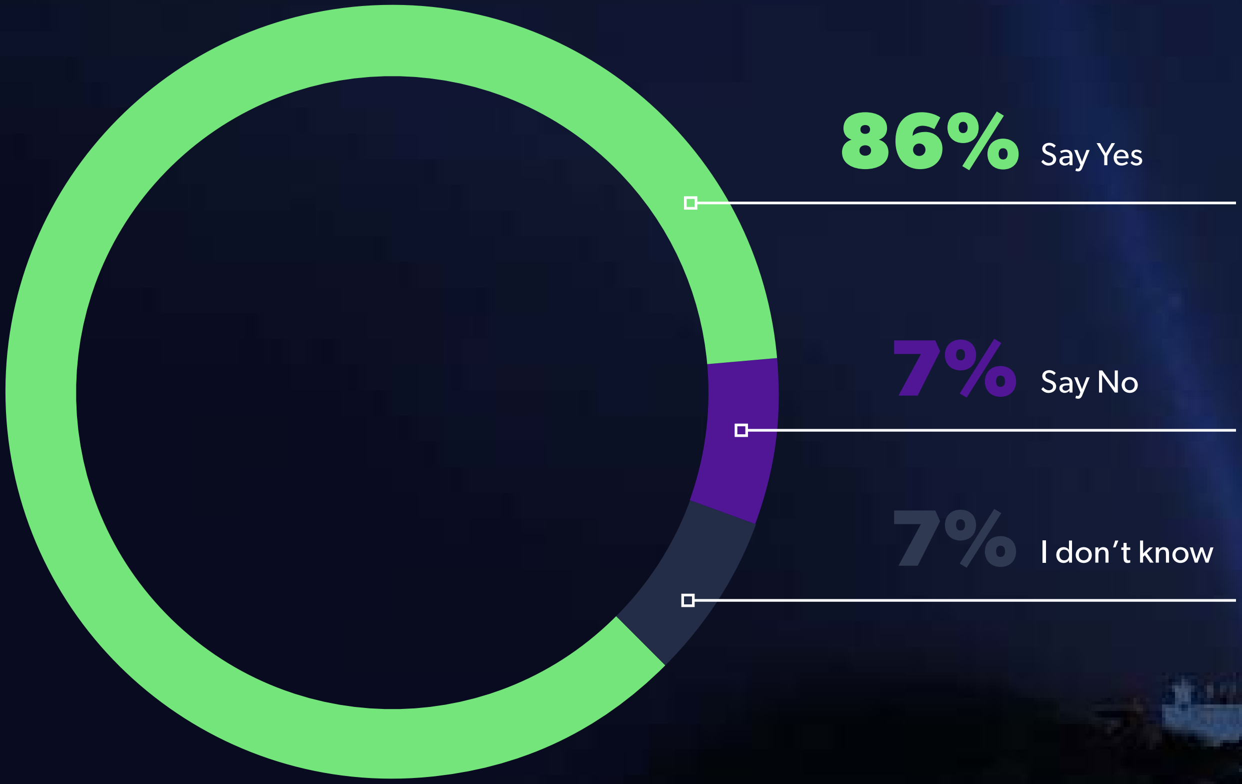
CYBERSCOOP | FEDSCOOP

MOVING TOWARDS SECURE ACCESS SERVICE EDGE

ALL RESPONDENTS

Enterprises are beginning to move to SASE (Secure Access Service Edge) security solutions. SASE applies secure access rules regardless of where applications, devices, users and workloads are located — at the network edge or in the cloud.

Is your agency currently moving toward a SASE security solution?



CYBERSCOOP | FEDSCOOP

CONCLUSIONS

- **Greater commitment to cyber resources** – The White House Cybersecurity Executive Order has had a catalytic effect in focusing attention on holistic cybersecurity. Half of federal IT leaders polled called the EO “greatly needed” — and another 30% called it “game-changing” — in getting agency leaders to commit resources to critical cybersecurity projects. Three in 4 respondents said Fiscal 2022 IT security budgets have increased to meet White House requirements, with 44% saying budgets had increased more than 10%.
- **Zero-trust maturity varies** – A majority of IT leaders, rated the maturity of zero trust measures across five key areas — for data, devices, identity and access, application workloads and network applications — as “traditional” or “advanced.” Fewer than 30% generally rated their configurations in those areas as “optimal,” suggesting that agencies have a long way to go to establish zero-trust environments, even with strategies in place.
- **Cyber risk gaps remain** – Federal IT leaders also indicated they are equipped to manage some security risks better than others. Two in 3 respondents said they’re able to continuously assess risks on traditional endpoints, but only half could do the same for mobile devices. And only 4 in 10 are able to provide dynamic granular access, verify cloud configurations, or secure data regardless of where it goes, suggesting agencies will need greater help in these areas.
- **Ongoing challenges** – The top challenges to establishing zero-trust environments are similar to the ones agencies face in modernizing as a whole: Complexity of their environment; conflicting IT priorities; the interdependency of existing technology; and limited budget and staff resources.
- **Embracing SASE** – Among other solutions to improve security, 86% of agency leaders said their agency is moving toward Secure Access Service Edge (SASE) solutions to better control applications, devices, users and workloads operating at the network edge. The growing focus on SASE suggests ways that newer technology solutions can help compensate for limitations in legacy systems.

CYBERSCOOP

CyberScoop is the leading media brand in the cybersecurity market. With more than 7.8 million monthly unique engagements and 273,000 daily newsletter subscribers, CyberScoop reports on news and events impacting technology and security. CyberScoop reaches top cybersecurity leaders both online and in-person through our website, newsletter and events to engage a highly targeted audience of cybersecurity decision makers and influencers.

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

PRESENTED BY CYBERSCOOP | FEDSCOOP UNDERWRITTEN BY Lookout