

CLOSING THE GAPS

IN FEDERAL

ENDPOINT SECURITY

More than half of agency IT officials worry about cyberattacks involving endpoint devices as a means of accessing agency networks. Yet many aren't taking advantage of technology they may already have to reduce their risks.

A new report looks at what matters most to federal CIOs and IT leaders in securing endpoint devices accessing their networks — and where the key gaps remain.

PRESENTED BY

cyberscoop | fedscope

UNDERWRITTEN BY

SAMSUNG

In a new survey of federal civilian and defense agency IT and cybersecurity decision makers,

CyberScoop & FedScoop identify:

- The top priorities and concerns IT officials face in securing mobile and endpoint devices capable of connecting to the internet
- The endpoint security features and capabilities most important to them to reduce vulnerabilities and improve mission effectiveness
- Where agencies stand in implementing various endpoint security strategies and tools
- The top challenges agencies face in implementing modern endpoint security
- Where agencies could use greater guidance

The state of endpoint security in federal government

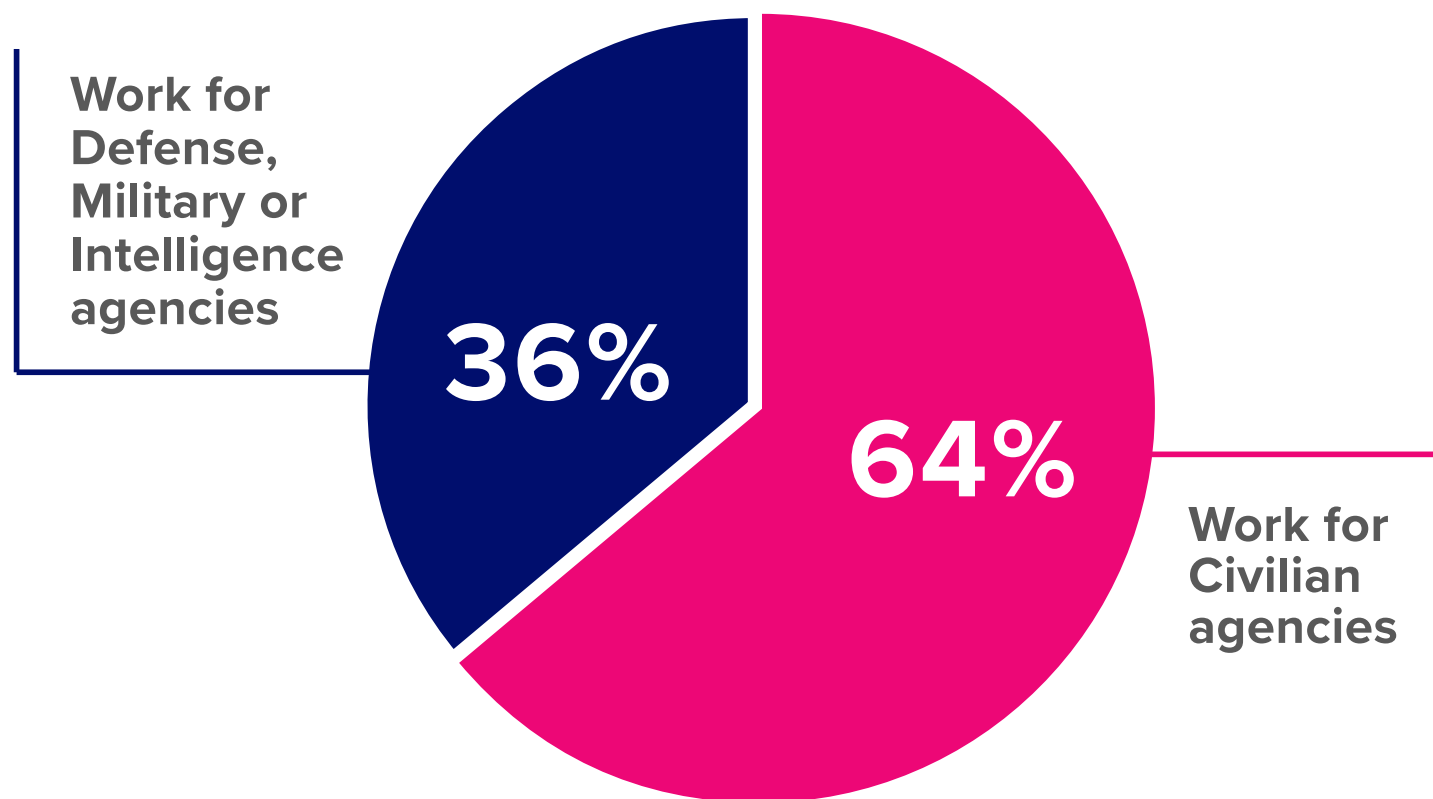
- Federal agencies are further along than is often assumed in implementing methods to secure smartphones, tablets, sensors, wearables and other endpoint devices accessing their networks. Defense/intelligence agencies are outpacing civilian agencies in embracing biometrics and alternative forms of authenticating users to improve endpoint security.
- However, the growing proliferation of devices accessing agency networks — including employees' personal devices — is driving up risks. More than half of agency IT officials are concerned about network attacks from endpoint devices.
- And while 6 in 10 say securing government-issued mobile devices is a top concern over the next 12-18 months, many may be overlooking technology they already have or own to address security concerns.

The endpoint security gaps federal IT/security officials still face

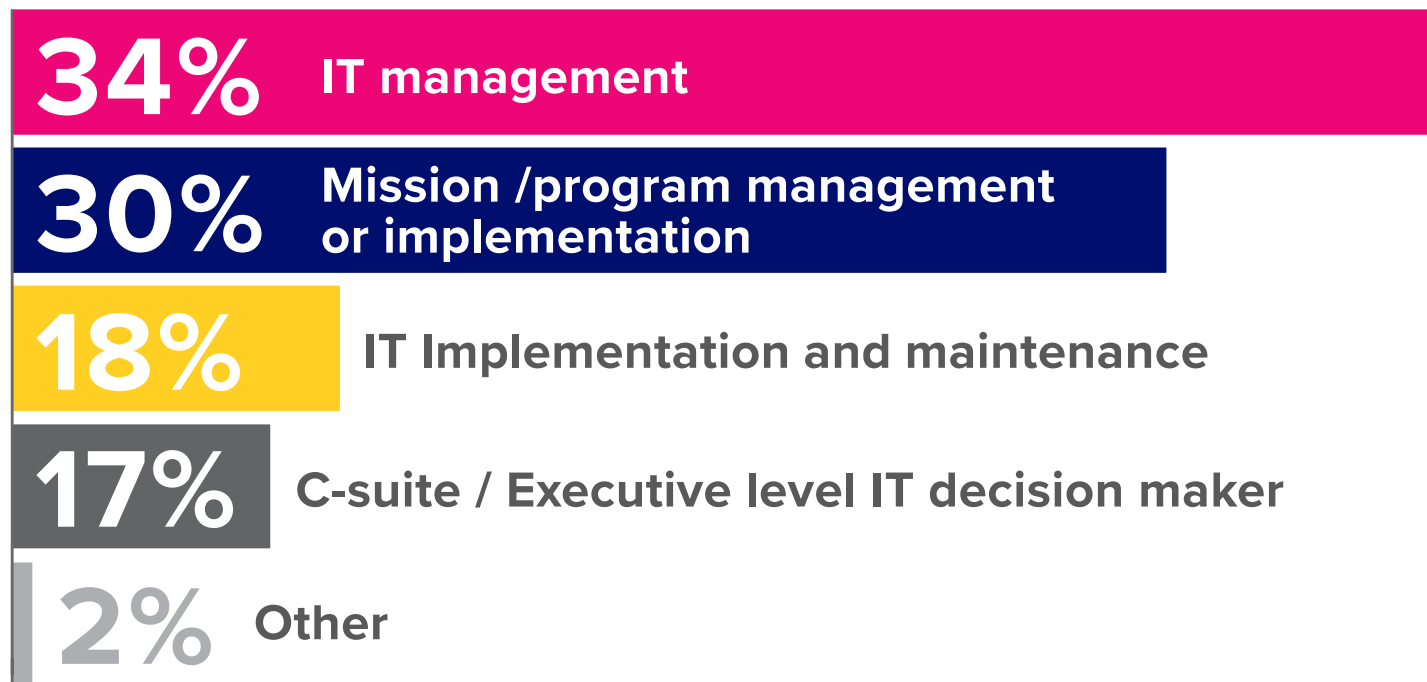
- **Top priorities:** Preventing cybersecurity breaches via endpoints — and improving the time it takes to identify and recover when security incidents occur — top the list of mobile security priorities over the next 12-18 months.
- **Top concerns:** Securing government-issued devices, addressing network and endpoint attacks and meeting endpoint security mandates are chief concerns over the next 12-18 months.
- **Top needs:** Agencies need the ability to centrally manage and configure mobile devices — and remotely lock down devices and recover data if a breach occurs. And they need greater guidance on emerging security threats, meeting federal security mandates and technical support for securing devices.

CyberScoop & FedScoop conducted an online survey of qualified federal government information technology and cybersecurity officials who have decision-making responsibility or influence regarding cybersecurity services, solutions, requirements, budgets or contractors.

Of the 167 survey respondents:



Federal job roles:



Top mobile security priorities in the next 12 – 18 months

among federal IT/security officials are:

Preventing cybersecurity breaches
from endpoint connectivity

64%

Improving time to identify and recover
when security incidents occur


46%

TAKEAWAY

Significantly more IT managers (61%) see improved identification and recovery time as a priority than their mission/program colleagues (34%) — suggesting potential alignment gaps within agency management.

Federal IT/security officials are also focusing on:

- Creating better management & monitoring dashboards **(42%)**
- Finding cost-effective endpoint cybersecurity solutions **(39%)**
- Simplifying secure configuration and management **(37%)**

4 in 10 

- Securing personal devices **(33%)**
- Reducing downtime by being able to quickly & easily reconfigure & reload user information on mobile devices **(37%)**

1 in 3 

— TAKEAWAY

While currently available technology makes it possible to configure mobile devices remotely using containers and other controls, it appears many organizations are not taking advantage of those capabilities.

Top mobile security concerns in the next 12 – 18 months

among federal IT/security officials are:

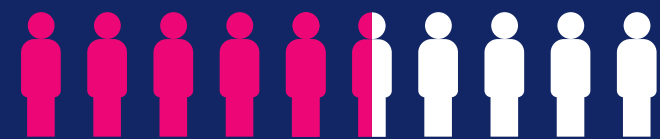
- Network attacks (62%)
- Securing government-issued devices (61%)

6 in 10

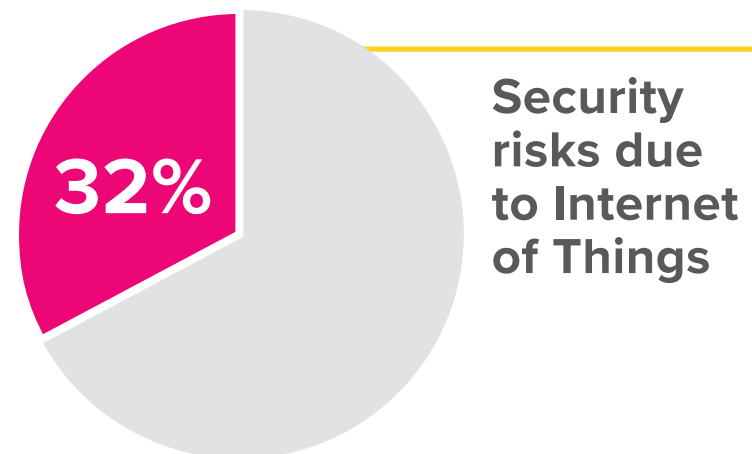
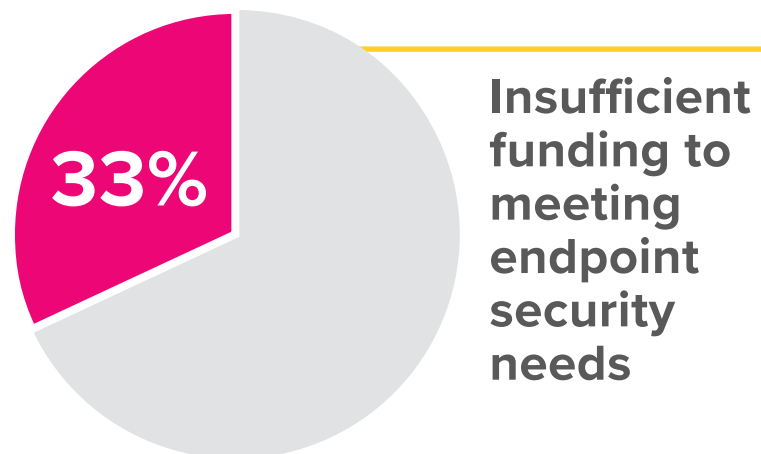
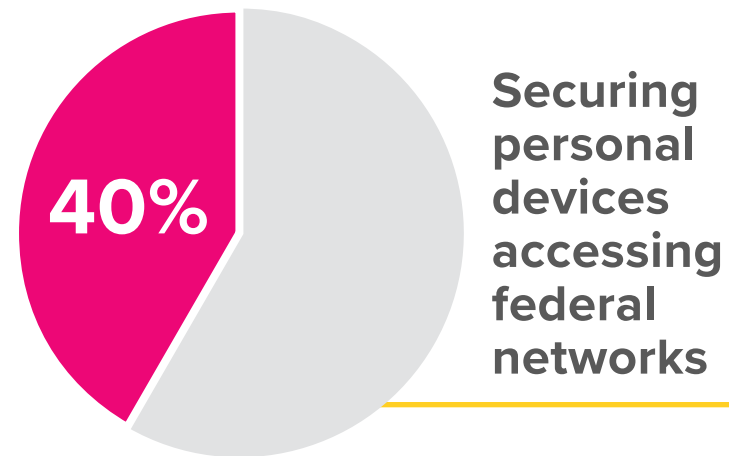
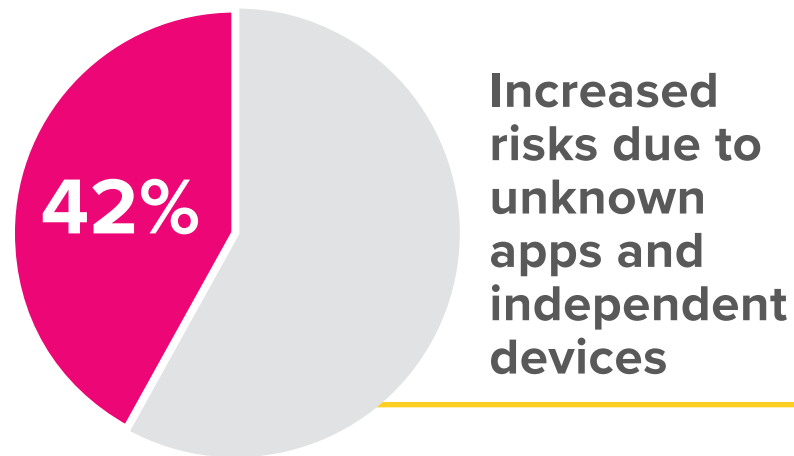


- Endpoint attacks (54%)

More than half



Federal IT/security officials express a number of concerns about the risks associated with endpoint devices, including:



TAKEAWAY

Significantly more IT managers (49%) see insufficient funding as a top concern than their mission/program colleagues (17%).

Federal IT/security officials are also concerned about:

Meeting federal endpoint security mandates

48%

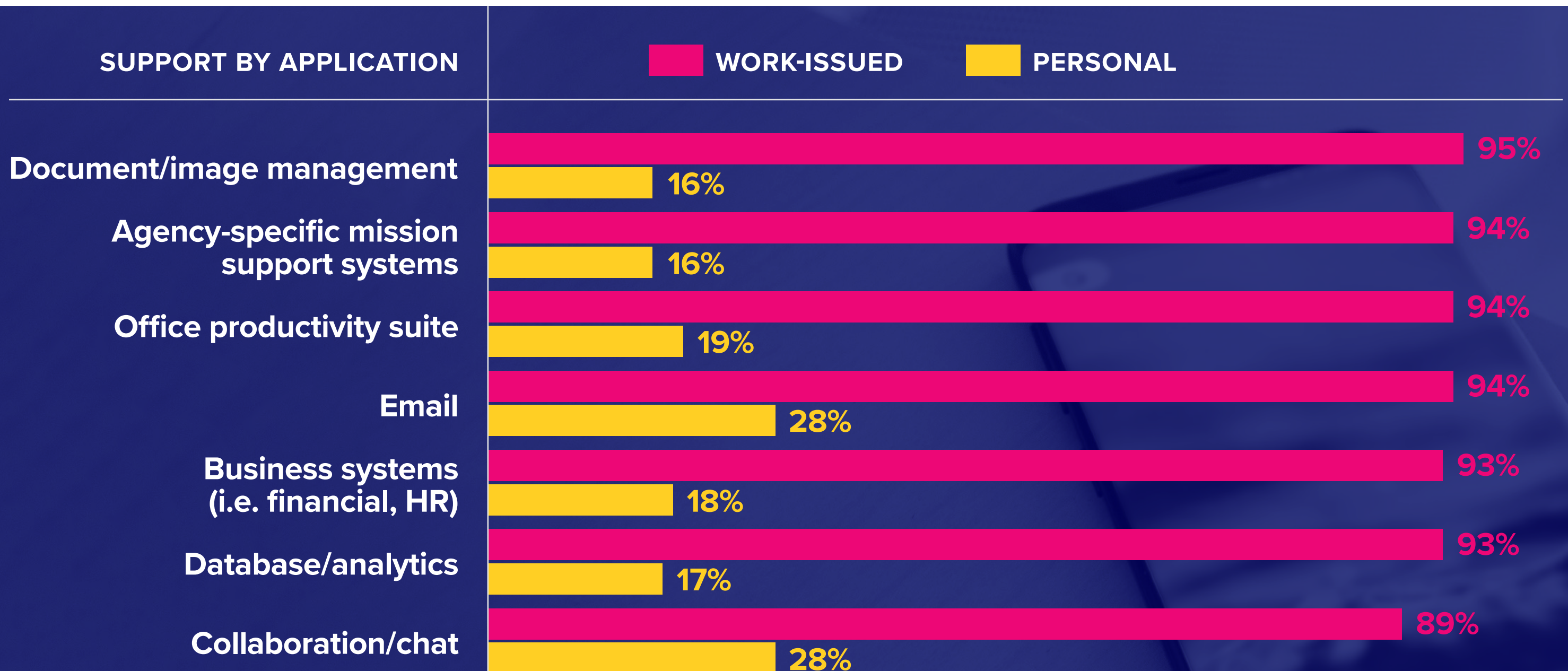
Lack of endpoint security guidance

29%

— TAKEAWAY

Agencies face a host of federal security requirements (such as FISMA, NIST 800-53, FIPS). Many of those mandates reflect outdated solutions or haven't kept up with changes in mobile technologies. Officials need more current guidance on emerging threats and practical technical guidance.

90% + of organizations **provide secure mobile access for work-issued devices.**
 But only about **one-quarter or fewer support** secure mobile access via workers' **personal devices.**



Question: For which of the following applications does your organization support secure mobile access? (Select all that apply.)

TAKEAWAY

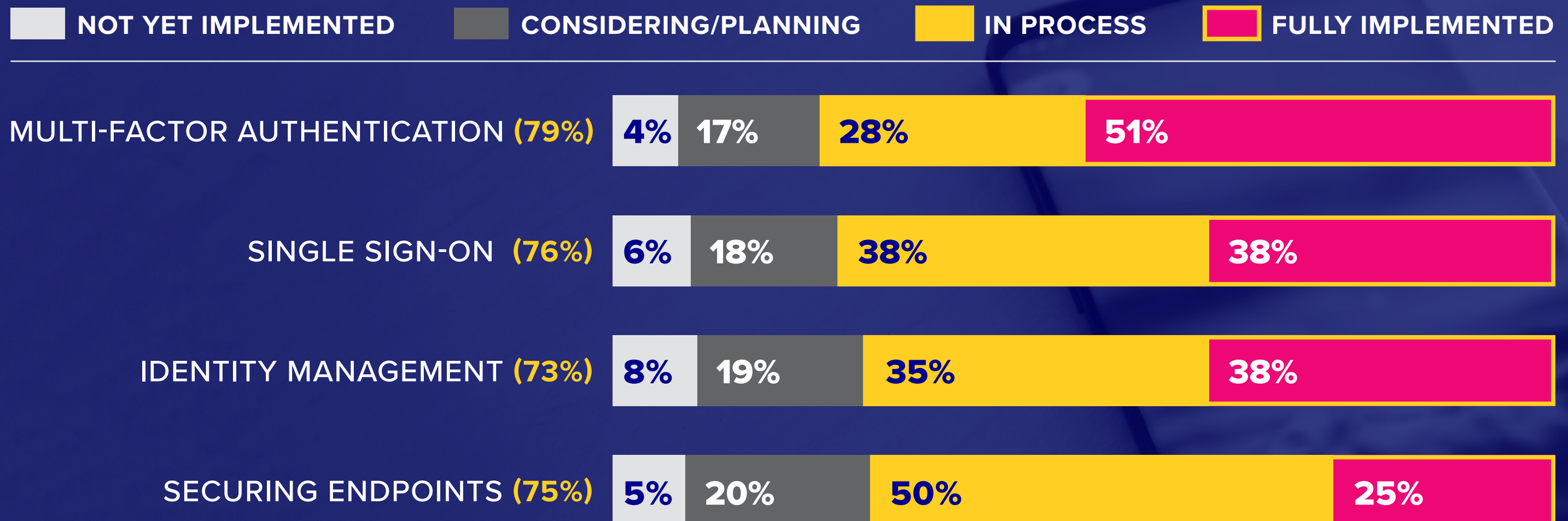
While roughly **20% of IT/security officials** say their **organizations support personal devices** accessing their networks, **40% expressed concern about securing personal devices**.

Another FedScoop survey* found among federal workers: **33% rely on personal laptops, 49% rely on personal smartphones and 74% rely on personal tablets for work**, even though federal agency IT managers don't support most of those devices.

This gap between the use of personal devices accessing federal networks and agency IT support for them points to a significant risk. The use of more modern devices and endpoint security practices, including containerization and centrally managed configuration tools, represent opportunities for agencies to improve their overall security posture.

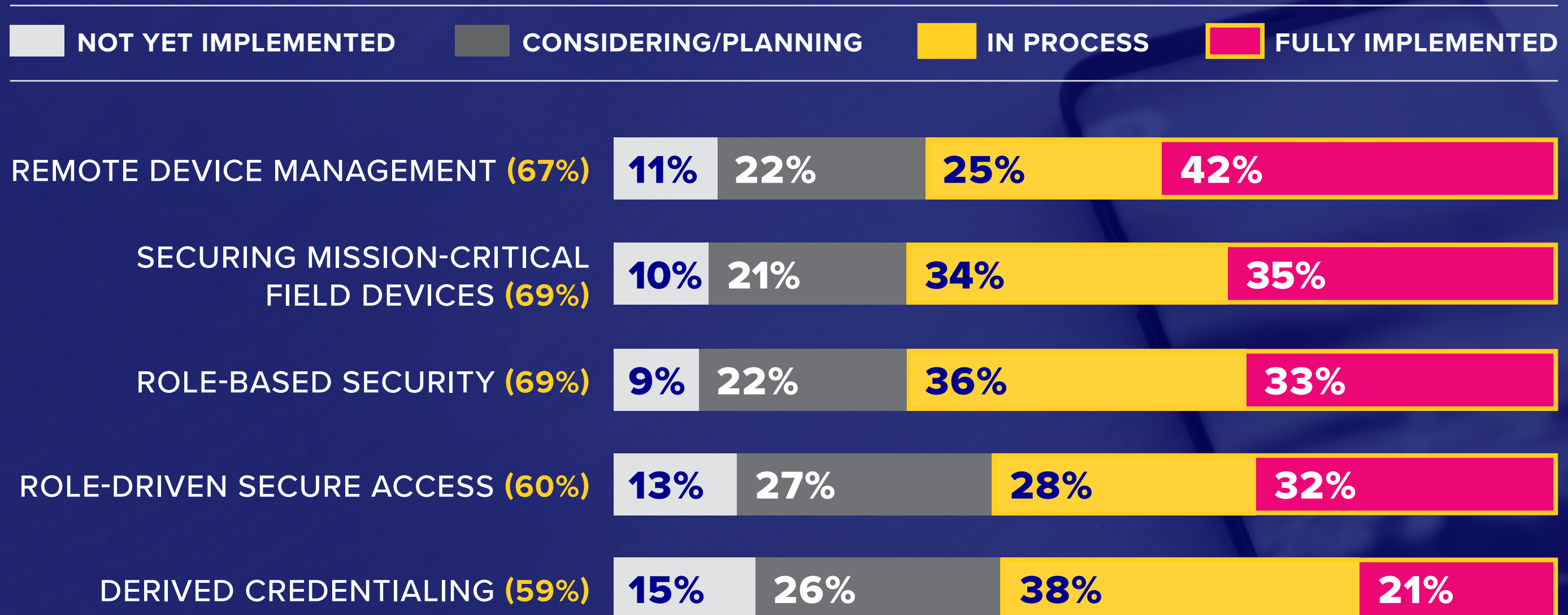
* FedScoop Workforce Productivity Study – July 2017

3 in 4 of federal IT/security officials have **implemented**, or are in the **process of implementing**:



Far fewer (25%) have fully implemented **securing endpoints** (using endpoint detection and response, network access control, end-to-end encryption, application control, etc.)

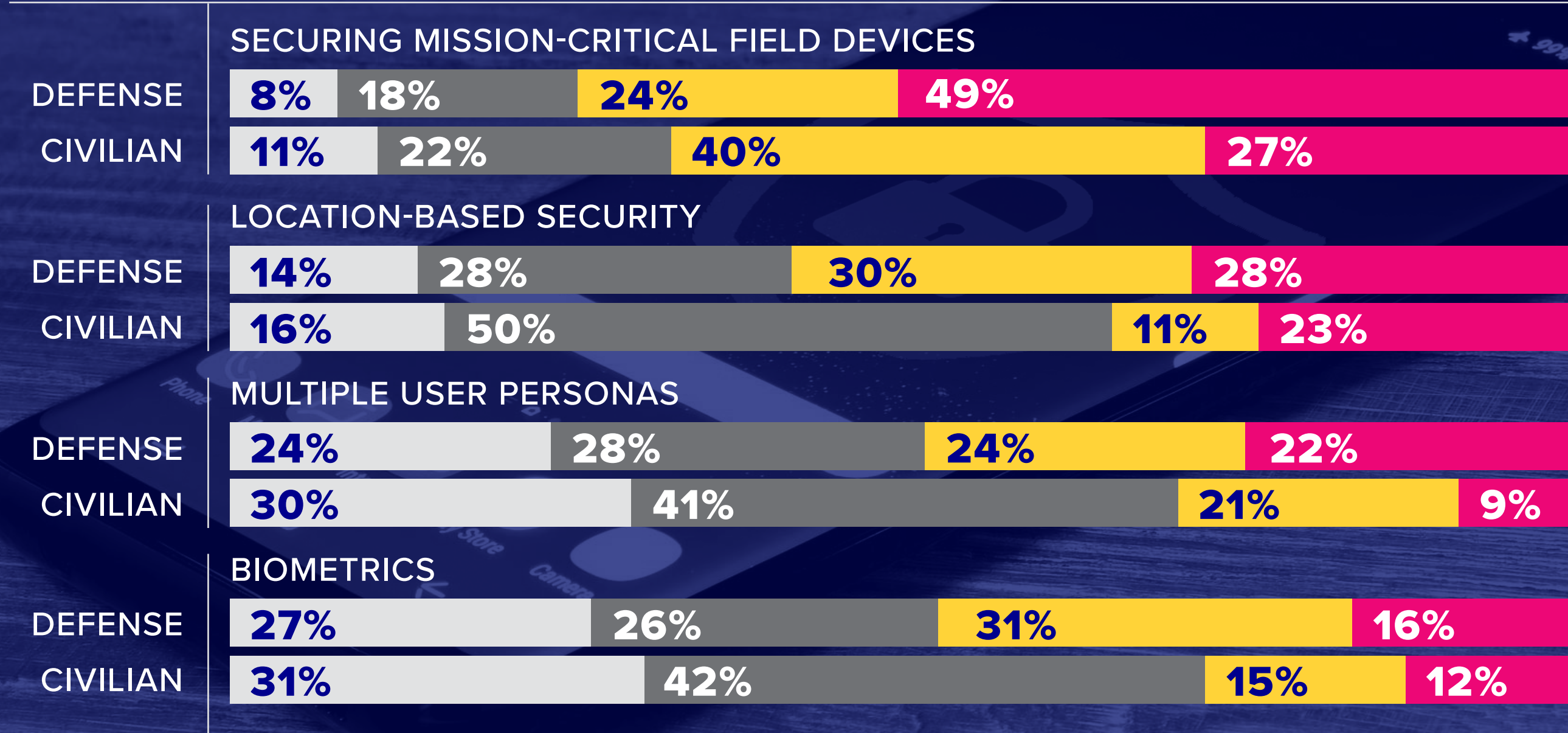
6 in 10 (or more) of federal IT/security officials **have implemented**, or are in the process of implementing:



Question: How far along is your organization in adopting the following? (Select all that apply.)

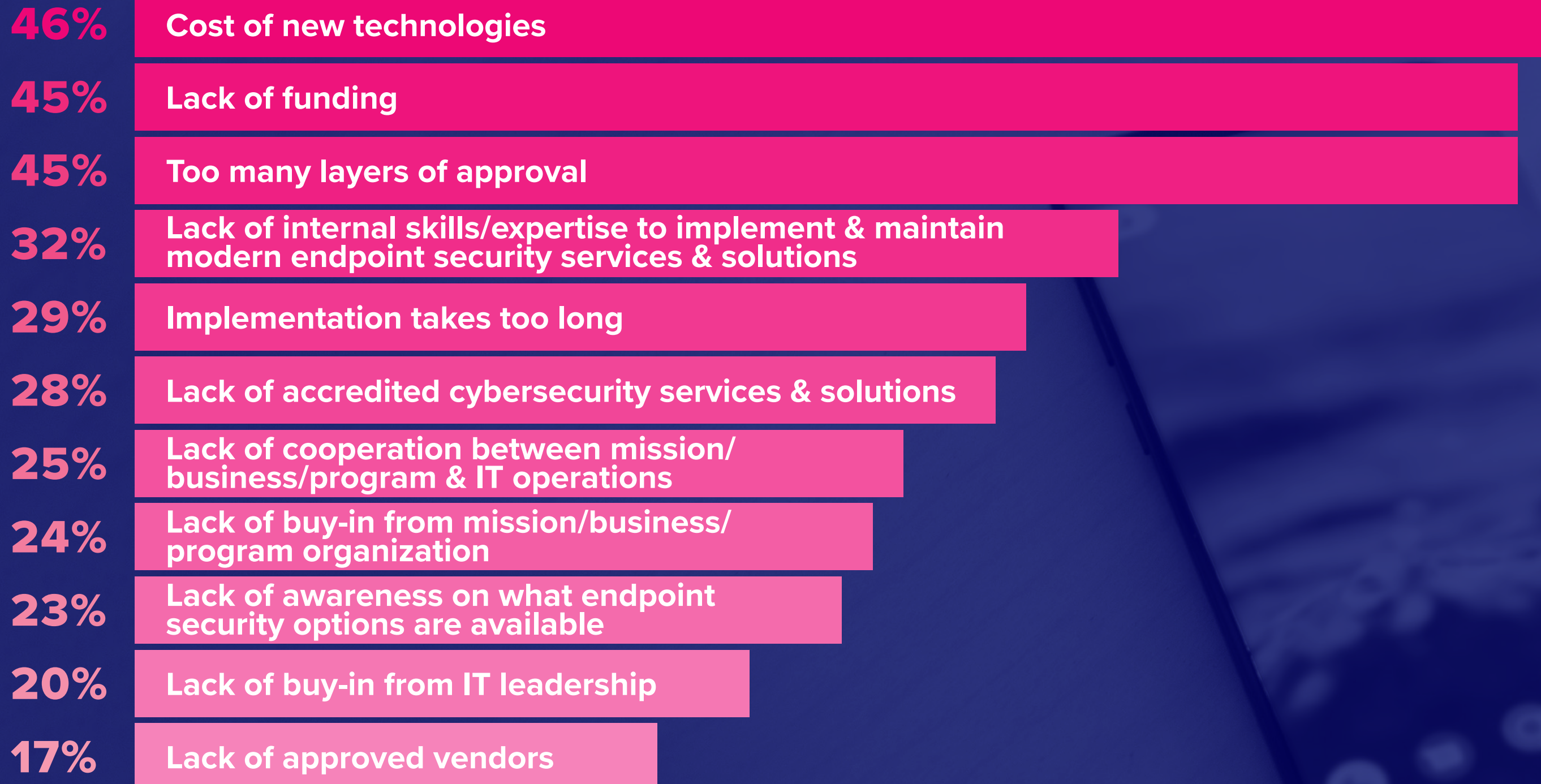
TAKEAWAY

Defense and intelligence agencies are further along than civilian agencies in implementing certain endpoint security approaches:



Question: How far along is your organization in adopting the following? (Select all that apply.)

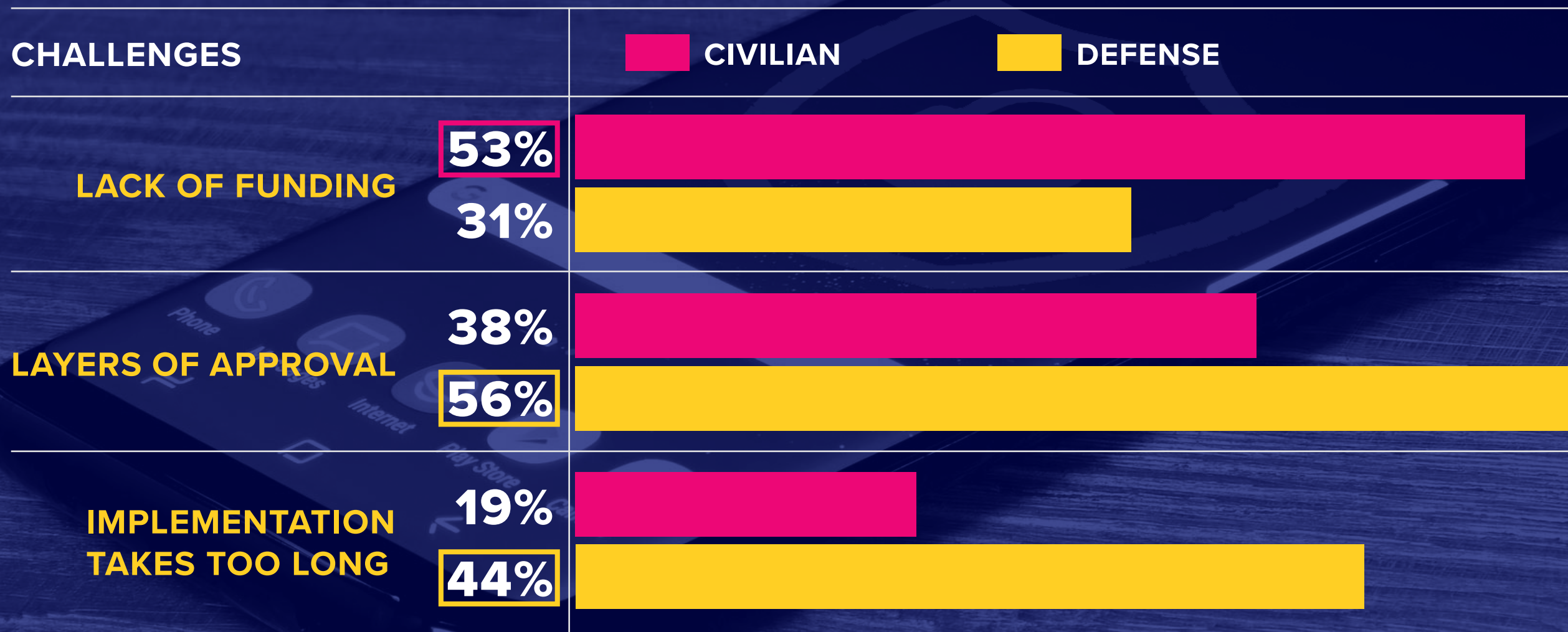
Cost, funding and approval processes — plus lack of internal skills — rank as top obstacles to implementing endpoint security.



TAKEAWAY

Civilian agency respondents are significantly more likely to cite **lack of funding** as an obstacle compared to their defense counterparts.

Defense/intelligence agency respondents cite greater challenges than their civilian counterparts regarding **layers of approval** and **implementation takes too long**.



Areas where organizations need guidance on endpoint security:

Staying ahead of emerging security threats (53%)

More than half



Meeting government-issued security mandates (39%)

Securing mobile devices (35%)

Providing secure, mission-critical field applications via mobile devices (33%)

More than 1/3



TAKEAWAY

Civilian agencies are significantly more likely than defense/intelligence agencies to need guidance on providing secure field applications and on derived credentialing.

Other areas where organizations need guidance on endpoint security:

Understanding endpoint security risks (30%)

Meeting NIST security guidelines (29%)

Derived credentialing (26%)

Allowing multiple user personas on devices (26%)

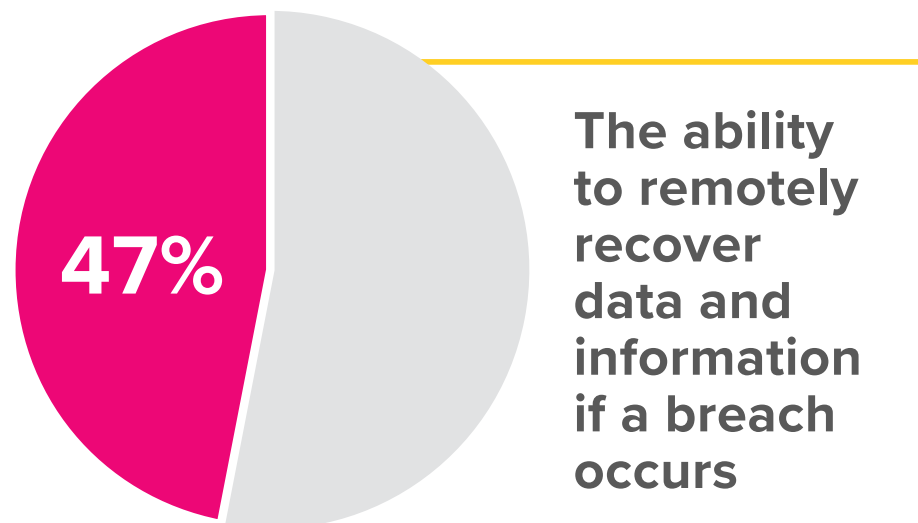
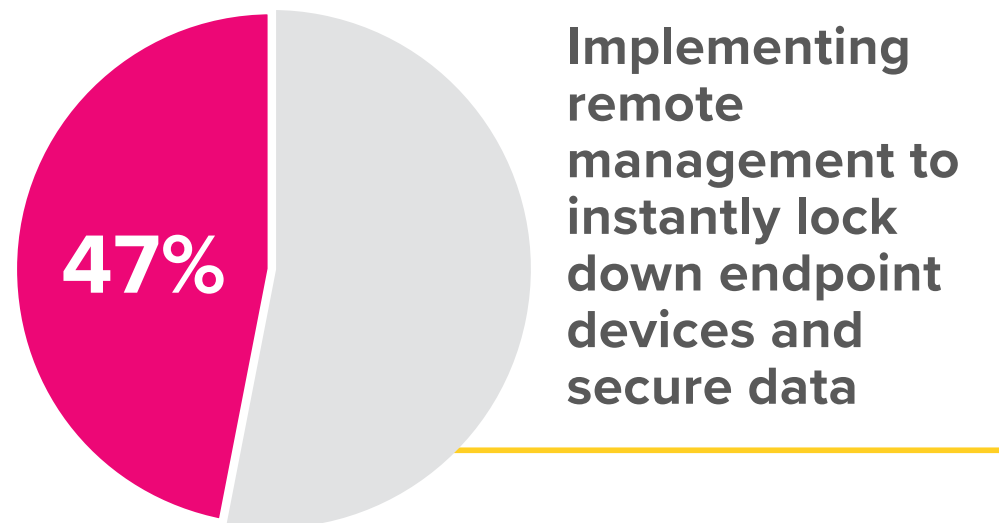
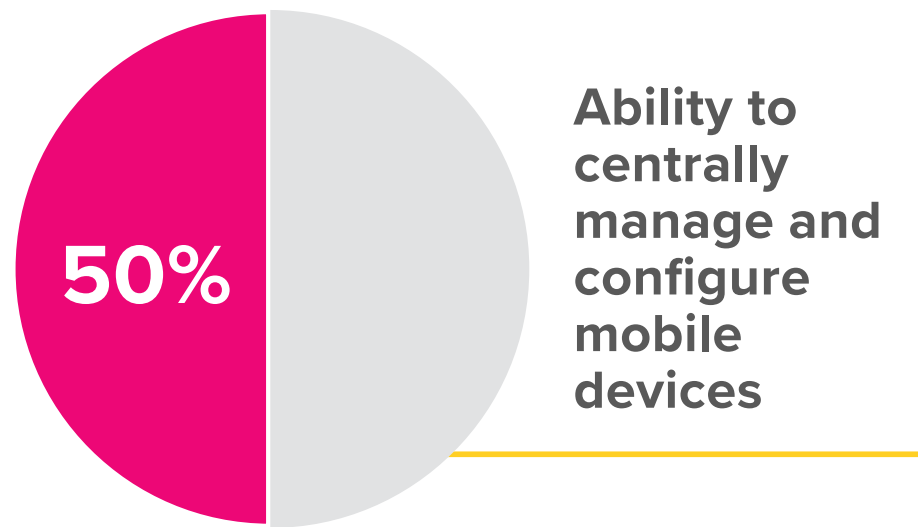
Multi-factor authentication (23%)

— TAKEAWAY

IT managers are significantly more likely than mission/program managers to need guidance for their organizations on meeting NIST guidelines and multi-factor authentication.

Features and capabilities that matter most for improving endpoint security

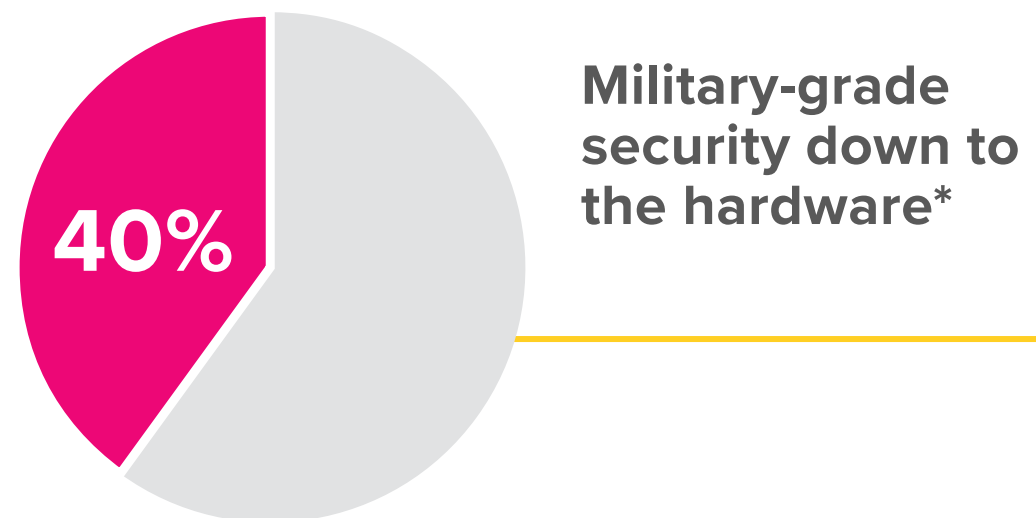
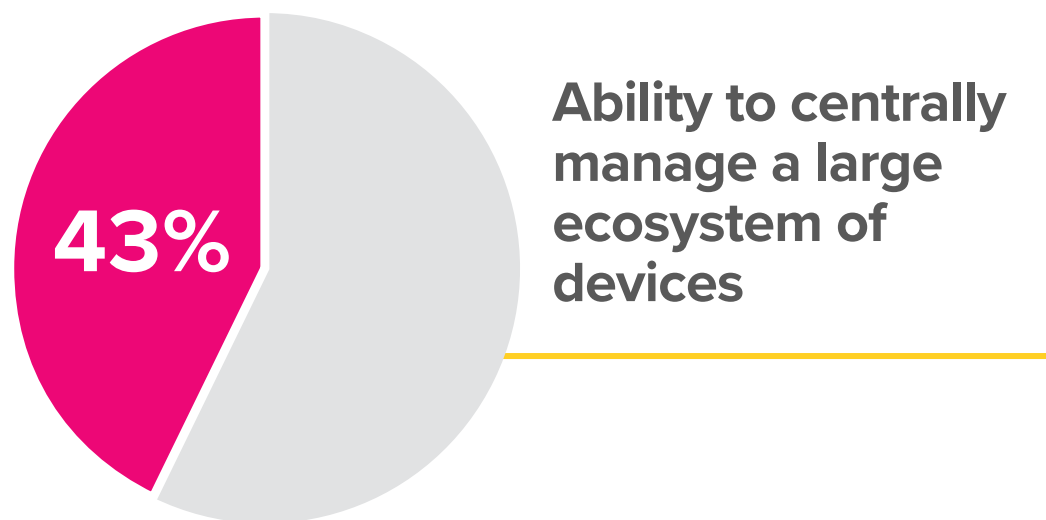
according to federal IT/security officials:



TAKEAWAY

Significantly more defense/intelligence IT/security officials (57%) said remote recovery of data was important to them than their civilian agency colleagues (38%).

Additional features/capabilities that matter most for improving endpoint security:



TAKEAWAY

Significantly more civilian IT/security officials (57%) said military-grade security down to the hardware was important to them than their defense/intelligence colleagues (30%).

* Applies security controls to the hardware, kernel, boot and application layers, not just the operating system.

1

Government agencies are making varying progress in implementing a number of proven methods for securing mobile and endpoint devices.

2

Agencies struggling with limited budgets could take greater advantage of technology they may already have — or is readily available in the commercial market — to improve endpoint security, such as affordable devices that support biometrics, derived credentialing and containerization.

3

Cost, funding and cumbersome approval processes are top obstacles to security implementation. But so is lack of internal expertise to implement modern endpoint security services and solutions.

4

Agency leaders must seek ways to reduce alignment gaps between the interests of mission/business managers seeking to improve productivity and service and the competing needs of IT managers responsible for reducing security risks.

ABOUT

cyberscoop

CyberScoop is the leading media brand in the cybersecurity market. With more than 350,000 unique monthly visitors and 240,000 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, events, radio and TV to engage a highly targeted audience of cybersecurity decision makers and influencers.

fedscope

FedScoop is the leading tech media brand in the federal government market. With more than 210,000 unique monthly visitors and 120,000 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

Sr. Vice President, Content Strategy

Wyatt.Kash@FedScoop.com

917-930-8531

PRESENTED BY

cyberscoop | fedscope

UNDERWRITTEN BY

SAMSUNG