THE GROWING NEED FOR **IDENTITY & ACCESS MANAGEMENT TOOLS** IN STATE & LOCAL GOVERNMENT

State and local agencies recognize the value of identity and access management (IAM) tools to improve IT security. But only a small number of IT leaders in a new survey say their agencies are taking advantage of them, even though most foresee growing demands for IAM solutions.

PRESENTED BY
statescoop

UNDERWRITTEN BY
okta

EXECUTIVE SUMMARY

State and local governments, like all organizations, face the challenge of handling more data, over more applications and devices, than ever before.

At the same time, agencies must navigate through competing demands to modernize legacy systems and strengthen their IT security posture, while also improving their IT services to employees and the public.

Across all those challenges: the need to know who's on their networks — and better control the data and applications they can access. Stolen and recycled passwords and inadequate access controls continue to pose critical security risks across government. But the lack of modern controls also comes at a cost to agencies, by impeding the delivery of services to citizens and reducing the productivity of employees.

To better understand the state of identity and access management (IAM) practices, StateScoop surveyed state and local government information technology leaders to explore the extent to which agencies are capitalizing on IAM technologies.

The survey, underwritten by Okta, sought to identify what's behind their decisions to implement IAM solutions, the challenges they face and how IT leaders view IAM solutions as a tool for addressing security and improving the online experience of citizens and employees.

The study also explored how early, mainstream and late adopters of technology look at IAM solutions differently. Early adopters in this study, for instance, have realized something that mainstream and late adopters can learn from: Namely, modern Identity Access Management is no longer simply a productivity tool. It is a strategic differentiator for both IT modernization and cybersecurity.

EXECUTIVE SUMMARY

Among the key findings of the study:

- 72% of state government, and 62% of local government respondents view automating IAM tools/ services as essential to addressing their agency's IT security concerns.
- Two-thirds of state and local respondents said automating IAM tools/services will be essential in efforts to adopt cloud computing services.
- Six in 10 mainstream technology adopters expect the number of on-premises and cloud-based applications used by employees will grow next year; and 45% expect the number of citizen-facing applications they must support will also grow next year.
- Less than 30% of state and local government respondents have implemented IAM tools or solutions.

The limited adoption of modern identity access management technologies puts agencies at a heightened risk of data breach — and points to a significant opportunity gap.

Agencies leaders appear to understand the value of IAM tools but only a minority of them are currently taking advantage of them.

EXECUTIVE SUMMARY

The need for modern IAM solutions is likely to grow as agency leaders contend with other IT demands, officials report.

Among other findings:

- One in 4 agency state and local respondents said their agency IT organization manages more than 30 apps for employees requiring sign-on privileges; 7 in 10 support five or more citizen-facing apps.

- Yet roughly half of state and local government respondents report their agencies have yet to begin implementing single sign-on technology, which can reduce the risks of poor password practices.

- Meanwhile, 1 in 6 respondents say it currently takes 4 hours or more to disable user access privileges, suggesting many state and local agencies face continuing risks of data exfiltration by departing employees.

The reasons behind the limited implementation of modern IAM solutions vary. Mainstream technology adopters and late adopters cite competing IT priorities and a lack of IT staff expertise. Early adopters point more toward the added complexity associated with IAM solutions and data integrity concerns.

At the same time, government respondents see IAM solutions addressing a combination of IT issues, with the primary drivers for pursuing IAM tools/services being security/privacy best practices; reducing costs and increasing efficiencies; and enhanced user services and satisfaction.

Recommendations:

This report concludes with five ***"next steps"*** for state and local government agencies to secure their IT environment more effectively by leveraging IAM technologies.

WHO WE SURVEYED

- StateScoop conducted an online survey of pre-qualified state and local government IT decision makers in May 2018 about identity and access management (IAM) practices at their agencies.
- A total of 150 government executives completed the survey, including 103 from state government agencies and 47 from local, country or municipal agencies.

Breakout by **job title:**

19%	C-suite/executive level IT decision-maker
18%	IT/network/security/application management
15%	IT acquisition, implementation or maintenance
29%	Mission, business or program management
19%	Other (Finance, engineering, administration)

Breakout by **IT involvement:**

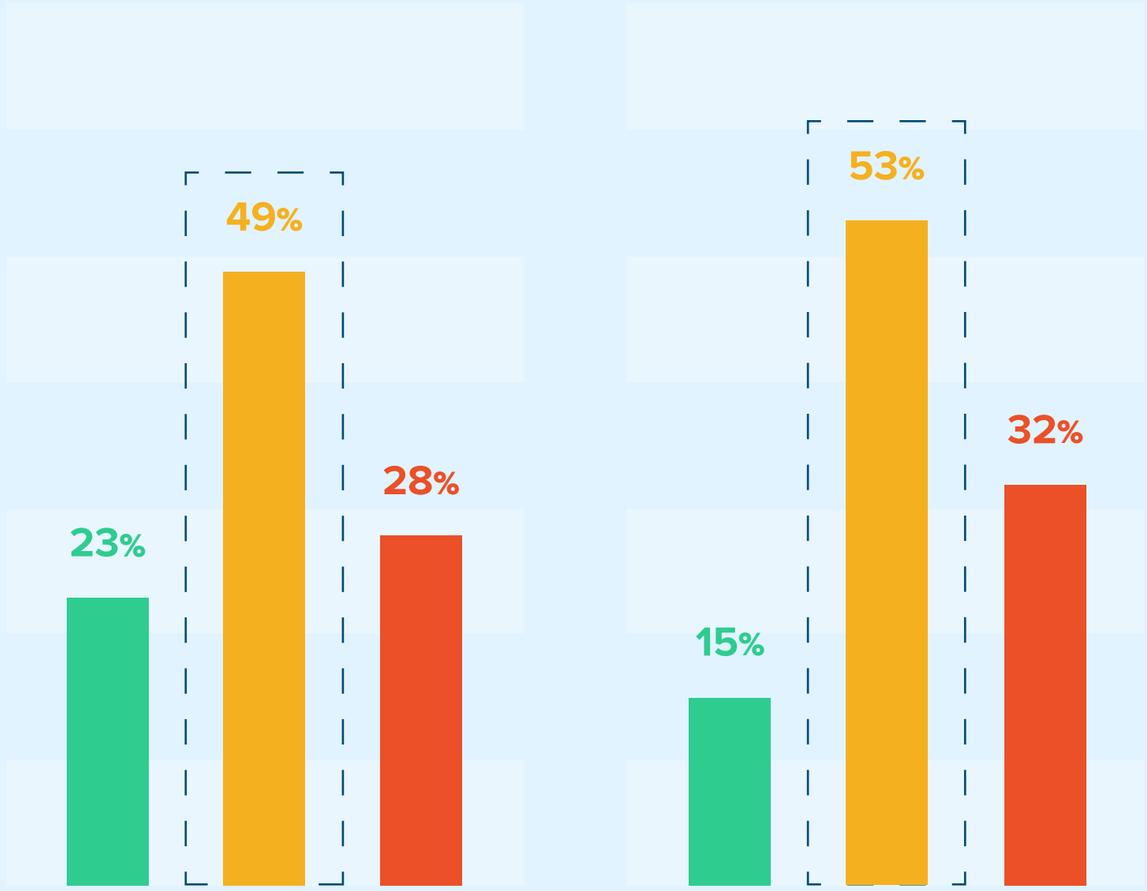
28%	Identify the need for IAM services, solutions or contractors
28%	Determine requirements, specifications or features of IAM solutions
21%	Allocate budget dollars for IAM or related IT solutions
35%	Evaluate, recommend or decide on IAM services, solutions or contractors
29%	Implement or manage IAM or related IT solutions
8%	Other governmental role

**Respondents could choose multiple roles*
**Percentages exceed 100% due to multiple responsibilities*

LEVEL OF TECHNOLOGY ADOPTION

One-half of state and local government respondents identify their agency as a mainstream technology adopter.

State agencies have a higher proportion of **early techology adopters (23%) than local agencies (15%)**. Early adopters showed significantly different views about IAM tools than late adopters.



State Government

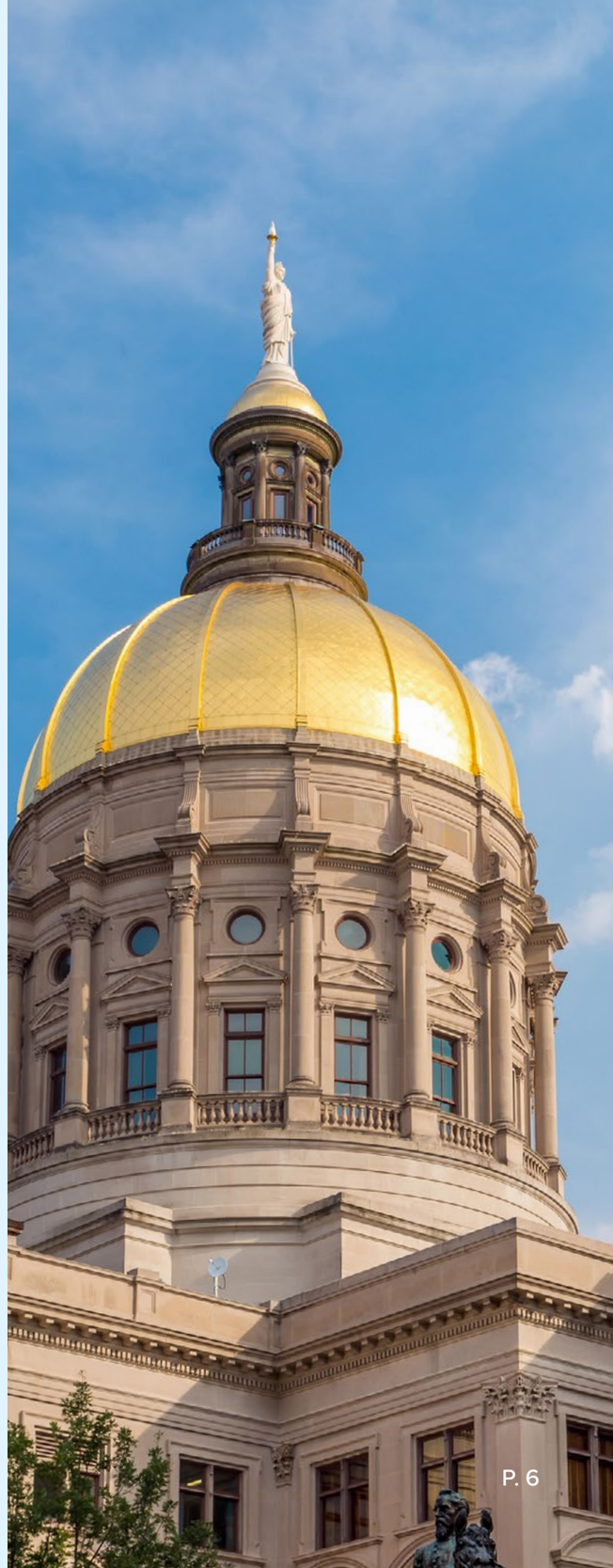
Local, County, or Municipal Government

Early Adopter

Mainstream Adopter

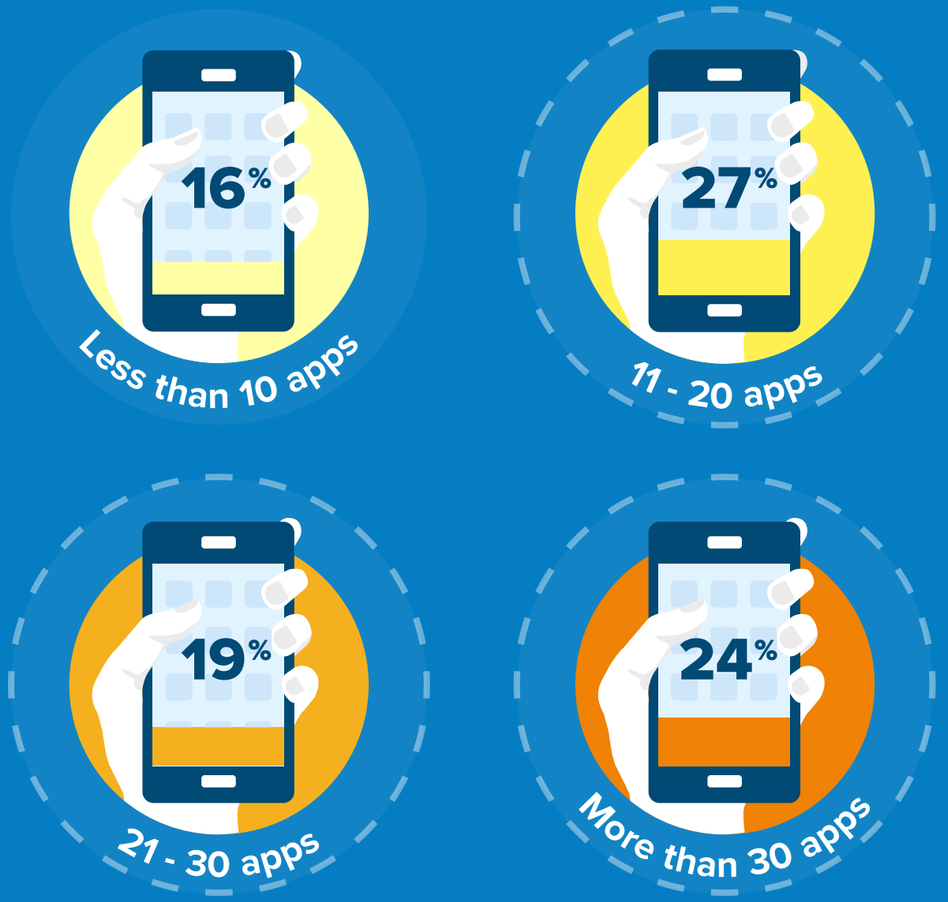
Late Adopter

Q: My organization's use of technology can be best described as:



GROWING EMPLOYEE DEMANDS FOR IAM

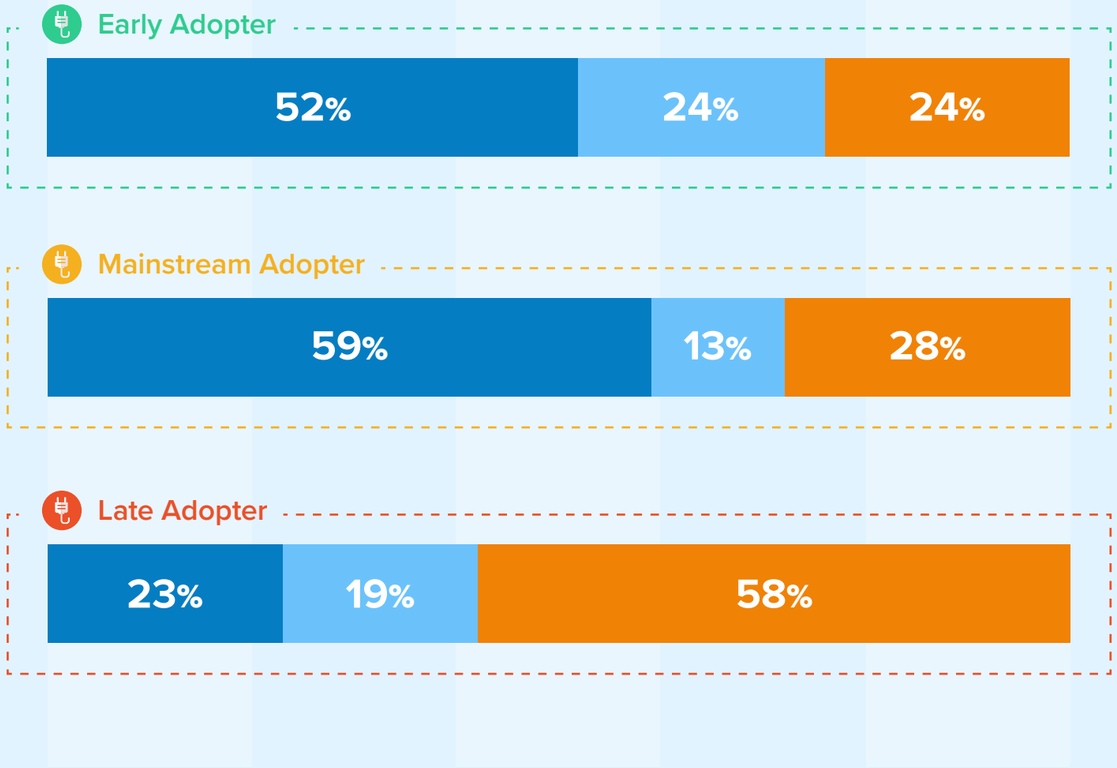
Agencies support a significant number of internal applications for employees and expect that number to grow in the coming year. **More than 7 in 10 respondents currently support more than 10 applications...**



14% don't know how many apps

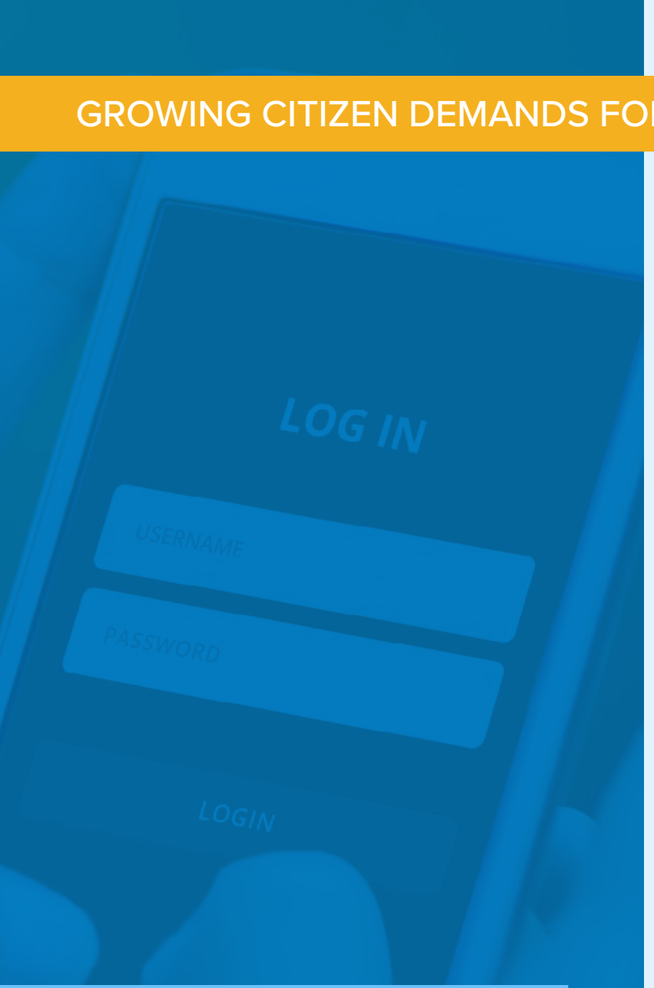
Q: How many employee applications or systems, requiring sign-on privileges, does your IT organization currently support (including both on-premises and cloud-based)?

...and a majority, including 59% of mainstream technology adopters expect the number of employee applications to grow next year, suggesting the need for IAM tools will only grow in importance.



Q: A year from now, do you expect that number to be...

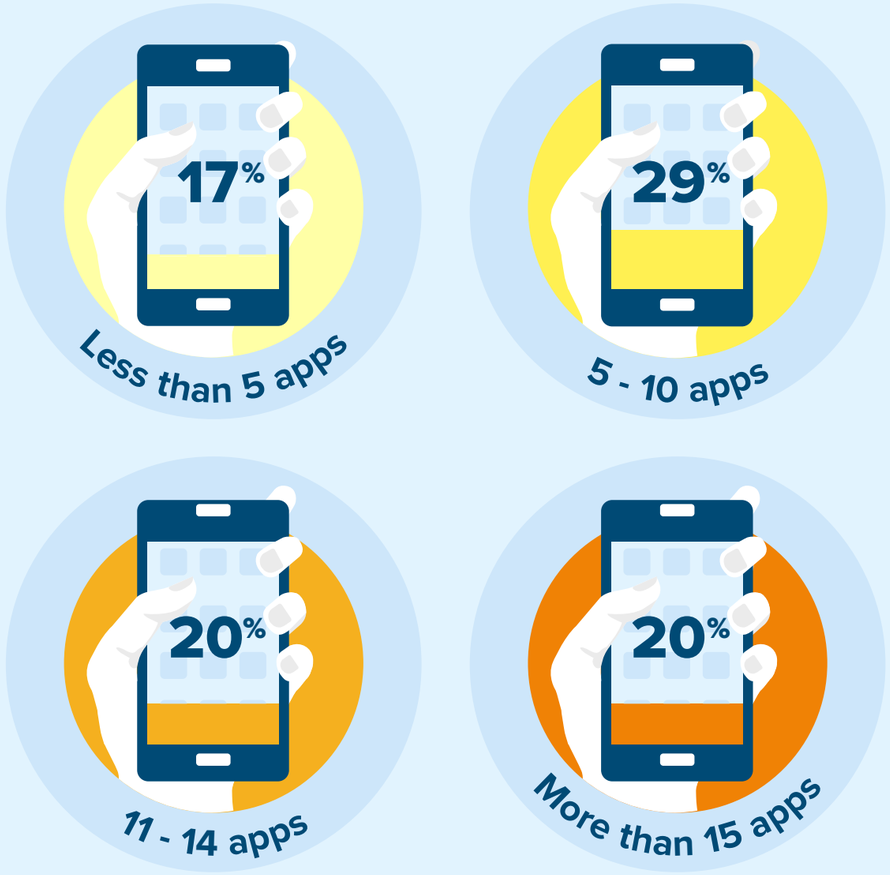
GROWING CITIZEN DEMANDS FOR IAM



Take-away: Given the volume of citizens logging on to multiple government applications, the findings suggest agencies need to ensure citizen -and constituent-facing applications deliver the kinds of user experiences the public is used to from consumer services.

statescoop

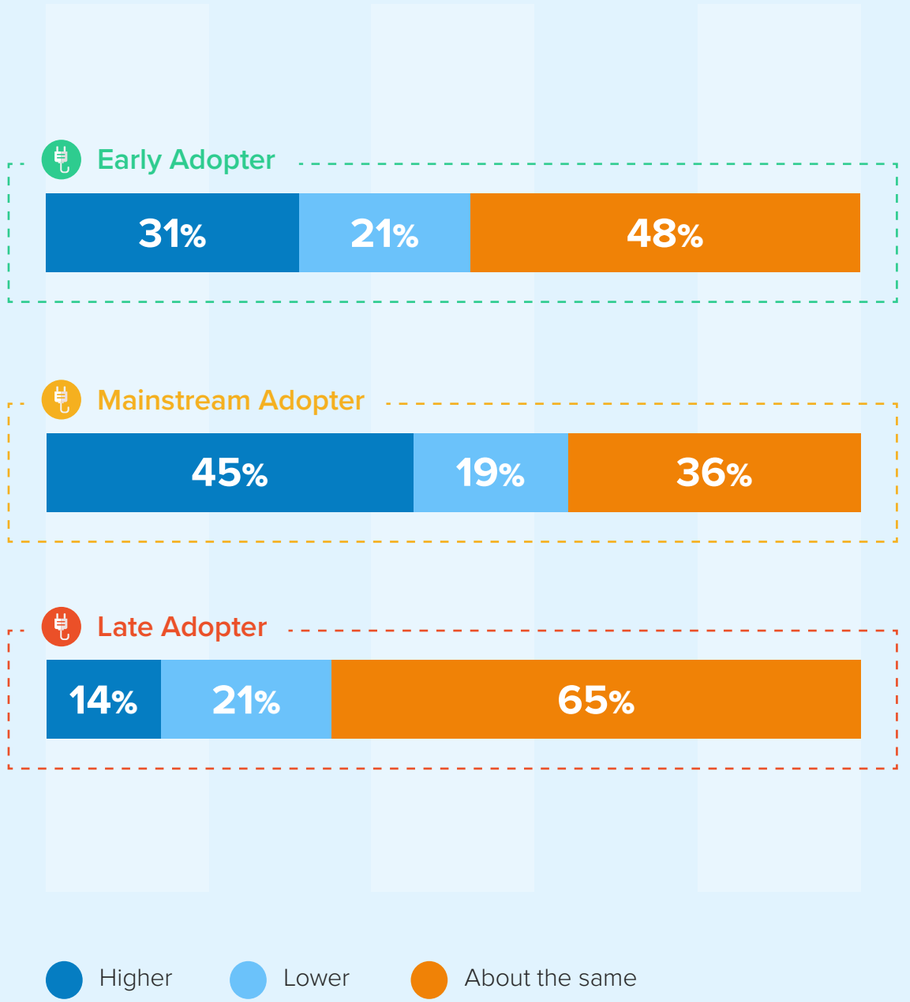
State and local agencies also report the need for more applications to deliver citizen services, further fueling demand for effective IAM tools. **69% of respondents** indicate they are currently supporting more than five citizen-facing applications...



14% don't know how many apps

Q: How many citizen-facing applications, requiring sign-on privileges, does your organization currently support (including both on-premises and cloud-based)?

...with **45% of mainstream adopters** and **31% of early adopters** expecting that number to increase in the next year.



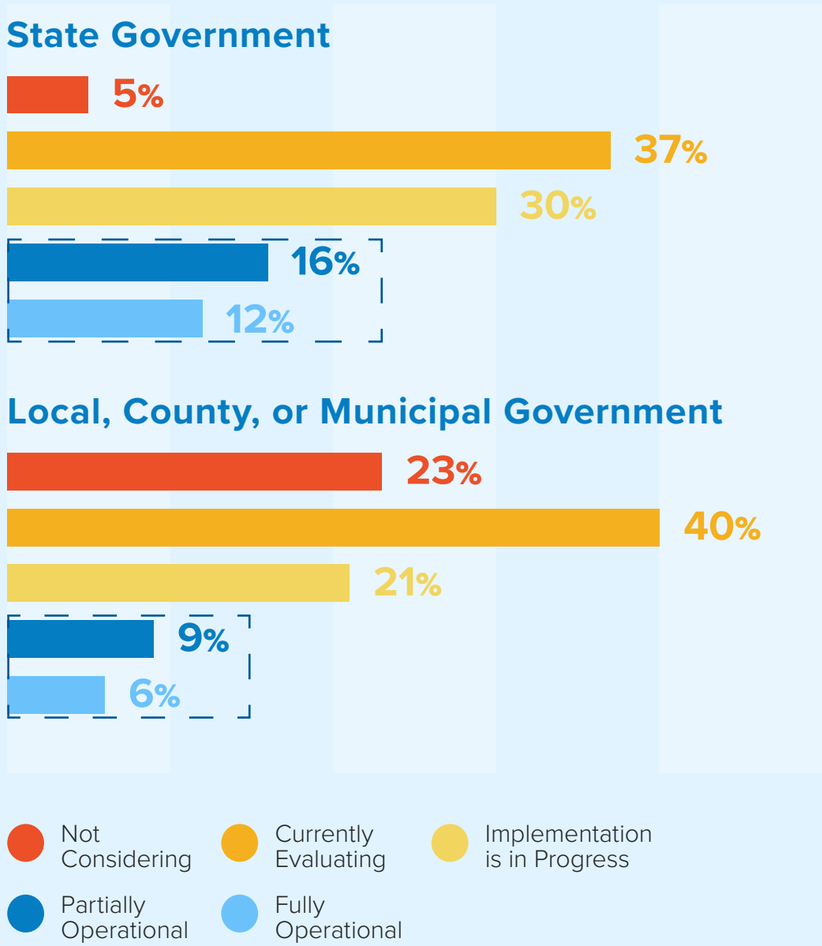
Q: A year from now, do you expect that number to be higher lower, or about the same?

LEVEL OF IAM TOOLS/SERVICES ADOPTION

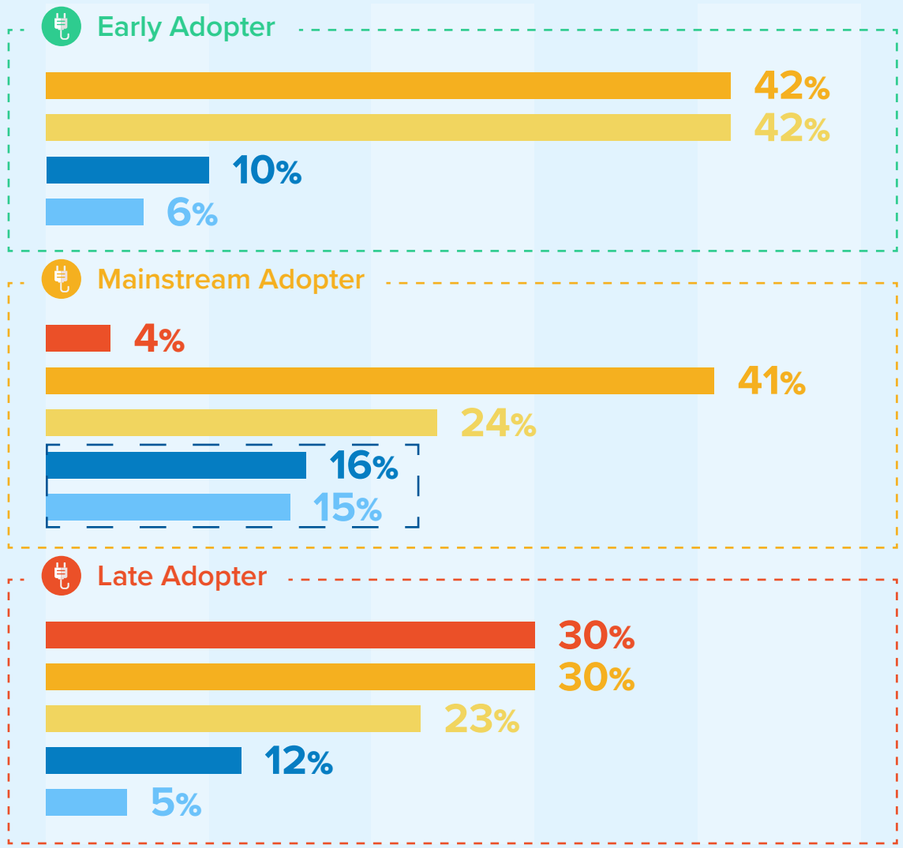
Take-away: High volume application use without IAM solutions encourages utilization of the same or recycled passwords across all of the user's applications. When one application experiences a breach, the risk to expose other applications using the same password increases. IAM takes the complexity out of passwords making organizations more secure.

statescoop

Despite evidence suggesting agency leaders recognized the value of IAM solutions, significant gaps remain. Only 28% of state respondents and even fewer (15%) of local respondents said they are fully or partially operational with their IAM tools.



The good news is a significant portion of agencies are either evaluating or in the process of implementing IAM tools. However, late adopters may not recognize the risks and rewards of delaying their IAM adoption; 30% of respondents indicate they are not considering these tools.

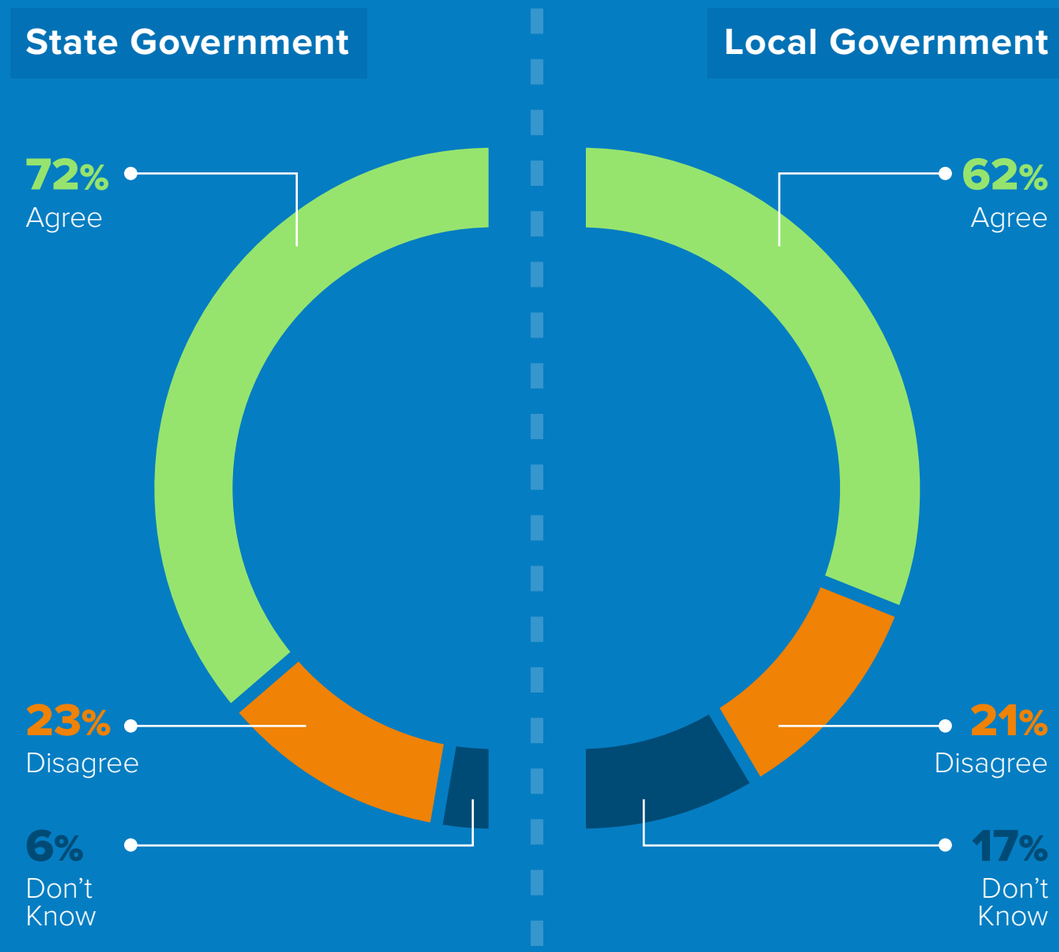


*Percentages don't add to 100% due to rounding

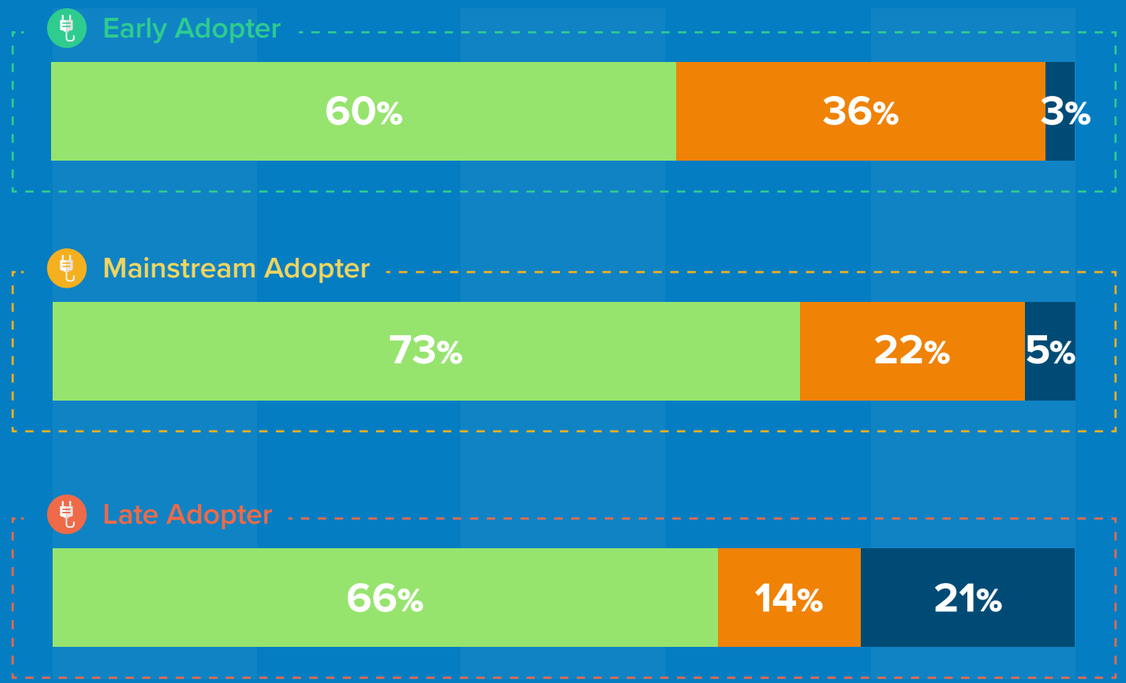
Q: To what extent is your organization using or considering IAM tools/services to centrally manage computer network access control?

RATIONALE FOR IAM: FUTURE SECURITY DEMANDS

6 in 10 local government respondents and **7 in 10 state respondents** indicated that automating IAM solutions is essential to addressing IT security concerns when working with contractors and outside collaborators.



Q: "'Federated identity' – the ability to automate management of identity information between your organization and others to facilitate collaborative or business initiatives – is essential to our IT security."

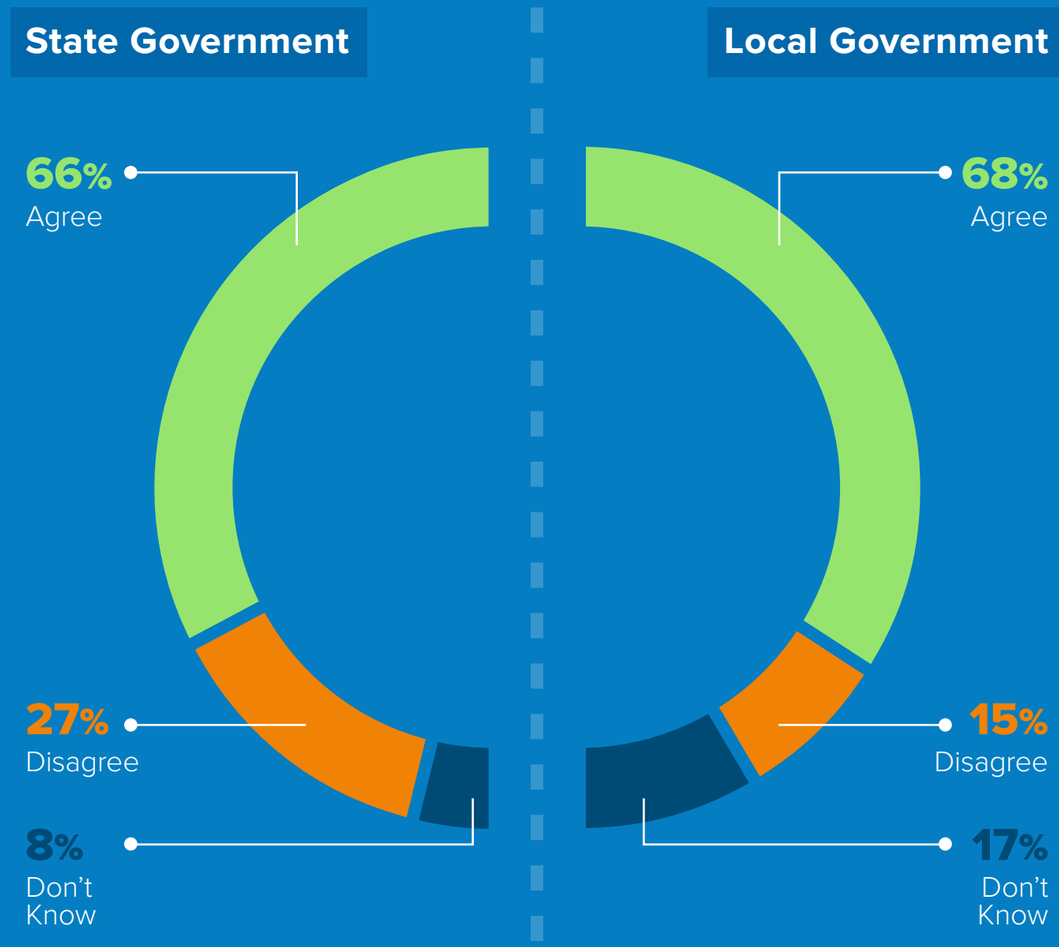


*Percentages don't add to 100% due to rounding

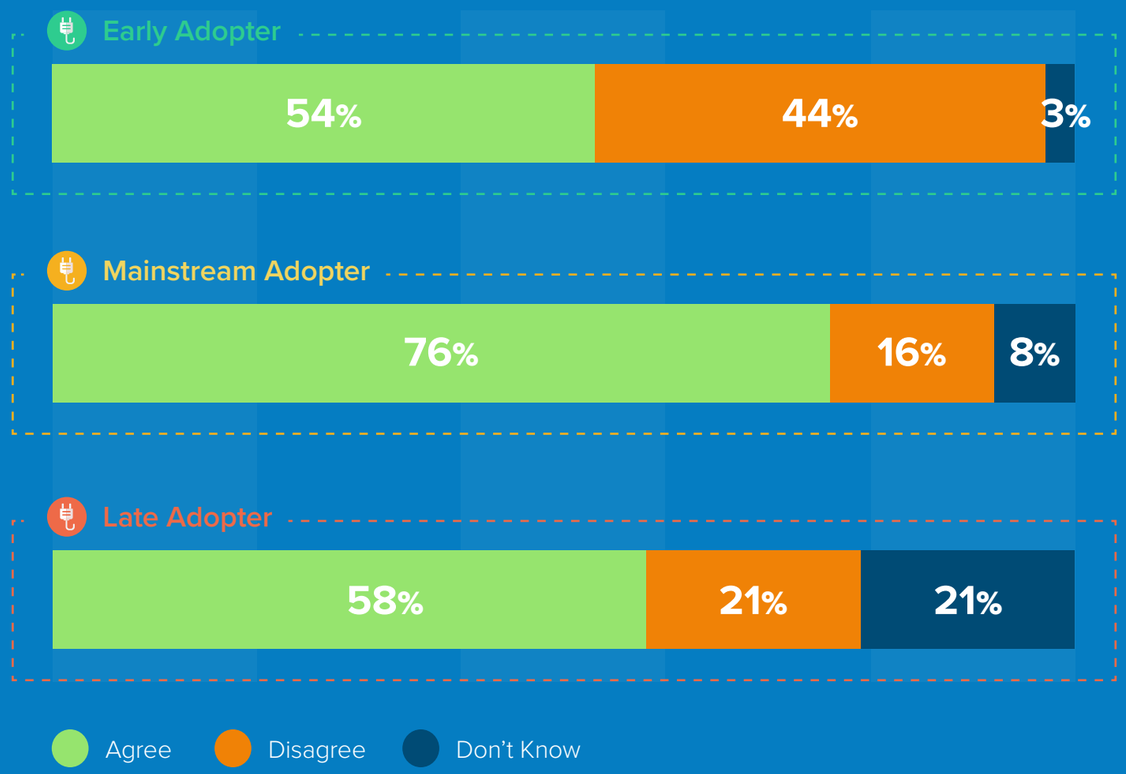
Take-away: *Government agencies exchange vast amounts of information across organizations and with third parties. The 2015 OPM federal data breach demonstrated the damaging impact of third-party vulnerabilities that IAM tools are designed to address.*

RATIONALE FOR IAM: FUTURE CLOUD EFFORTS

Two-thirds of state and local respondents indicated automating IAM tools and services will be essential to efforts to adopt cloud computing services.



Q: "IAM tools / services are essential to our efforts to adopt cloud computing services."

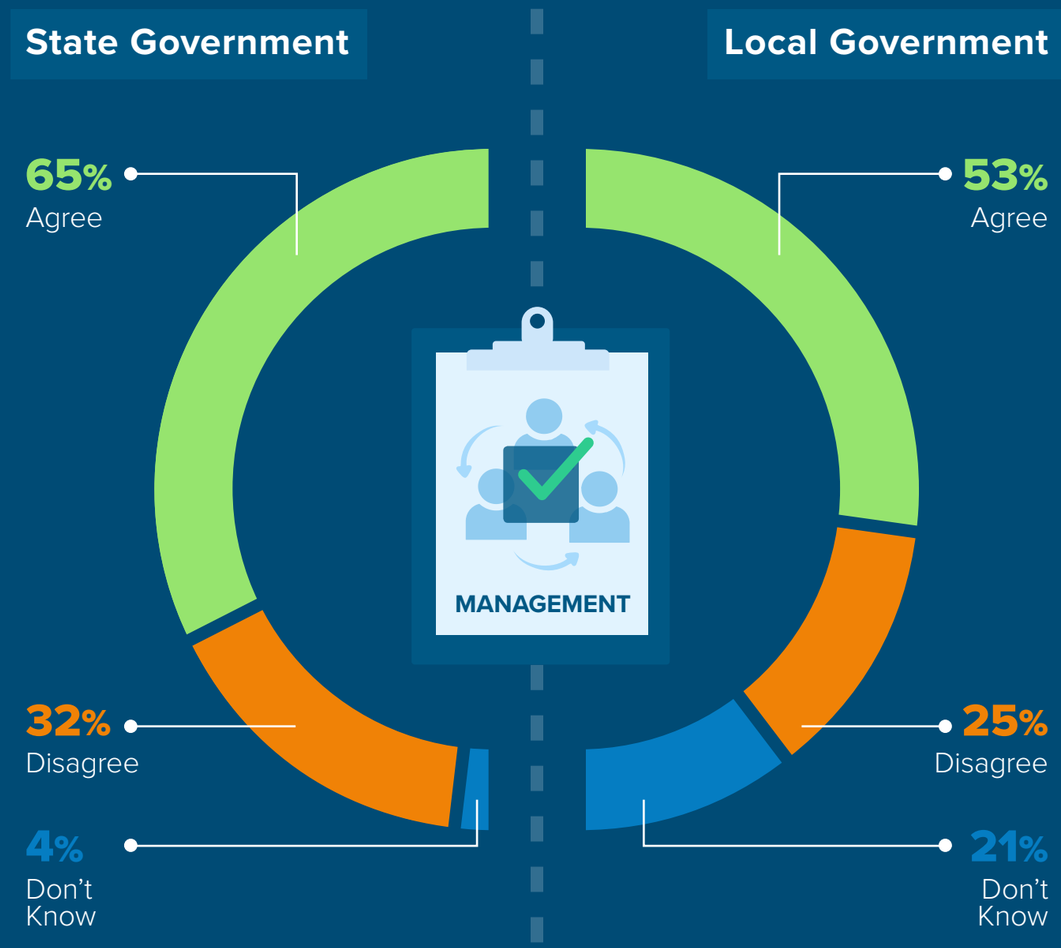


*Percentages don't add to 100% due to rounding

Take-away: *Having the right IAM tools in place also makes it easier, faster and more efficient for state and local agencies to transition to cloud computing.*

SUPPORT FOR IAM TOOLS: MANAGEMENT

Two-thirds of state and half local government respondents say that senior management understands the value of IAM.



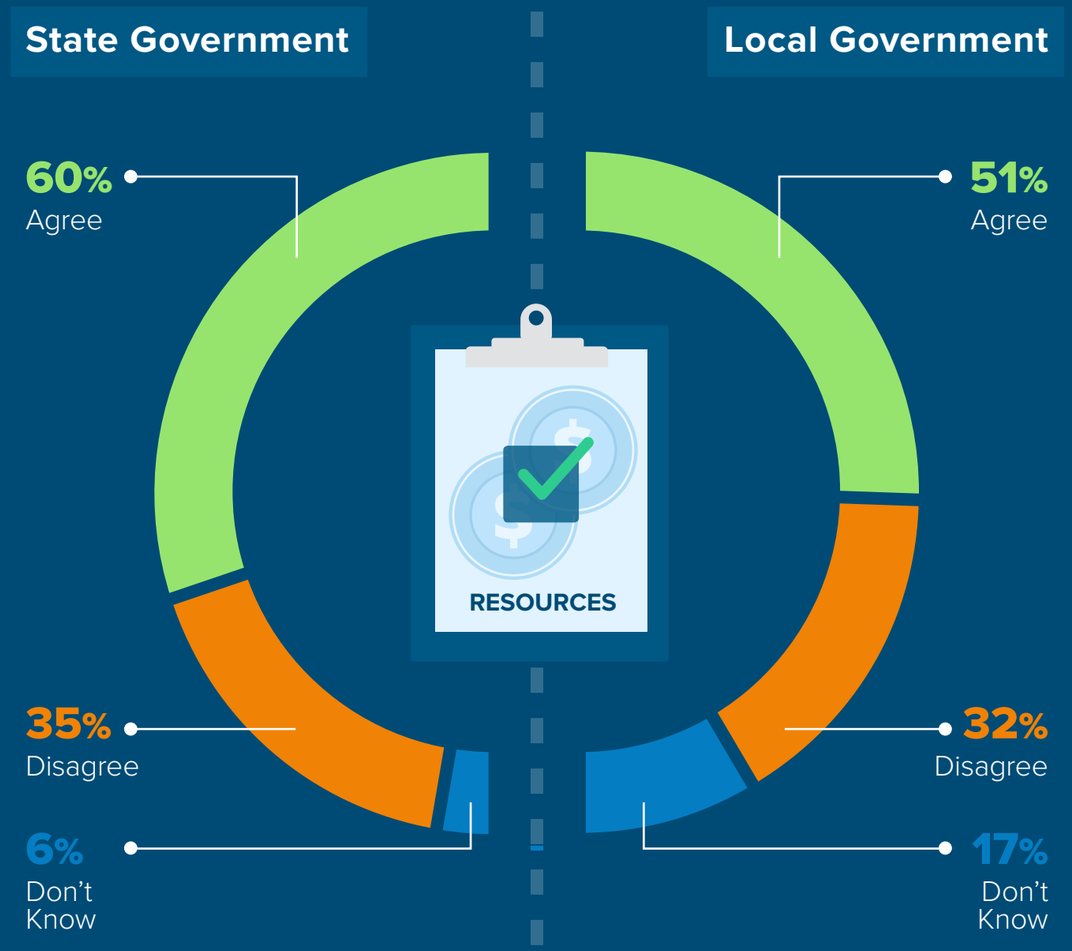
**Percentages don't add to 100% due to rounding*

Q: "My organization's senior management understands the value of IAM."

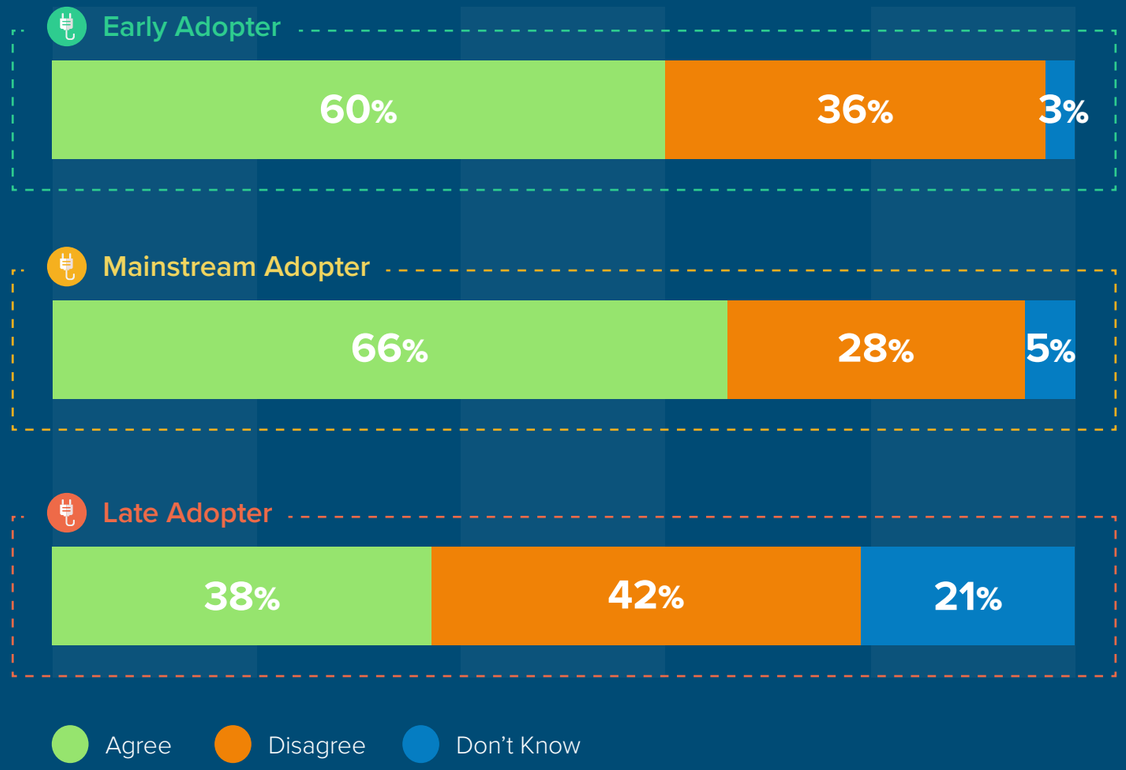
Take-away: *While management support for IAM tools is high, the study suggests other complicating factors are hampering the ability for IT leaders to fully implement these solutions.*

SUPPORT FOR IAM TOOLS: RESOURCES

While **more than half of respondents feel their organization provides the needed time, money or tools to manage IAM**, one-third of respondents say they lack these resources.



42% of respondents identifying as late technology adopters feel they don't have the needed resources to effectively manage an IAM strategy.

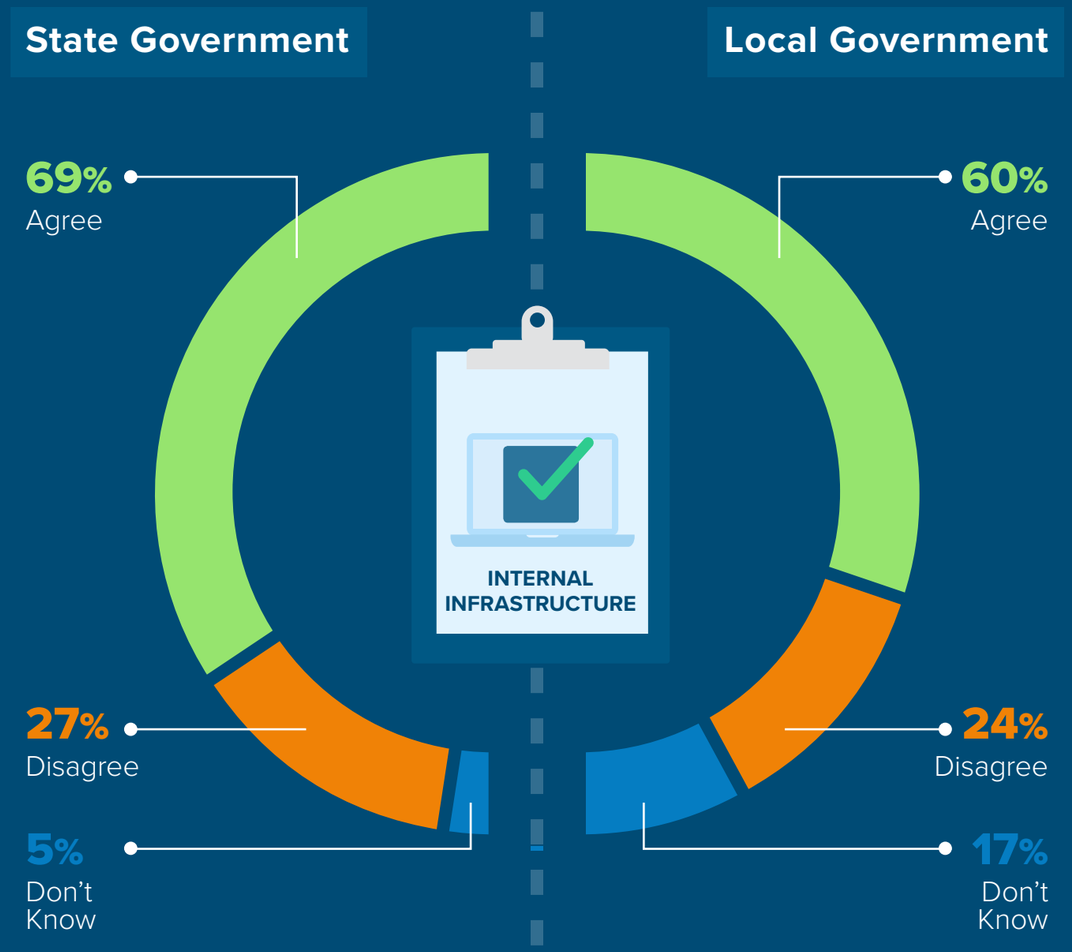


*Percentages don't add to 100% due to rounding

Q: "My organization provides the time, money, tools needed to effectively manage an IAM strategy."

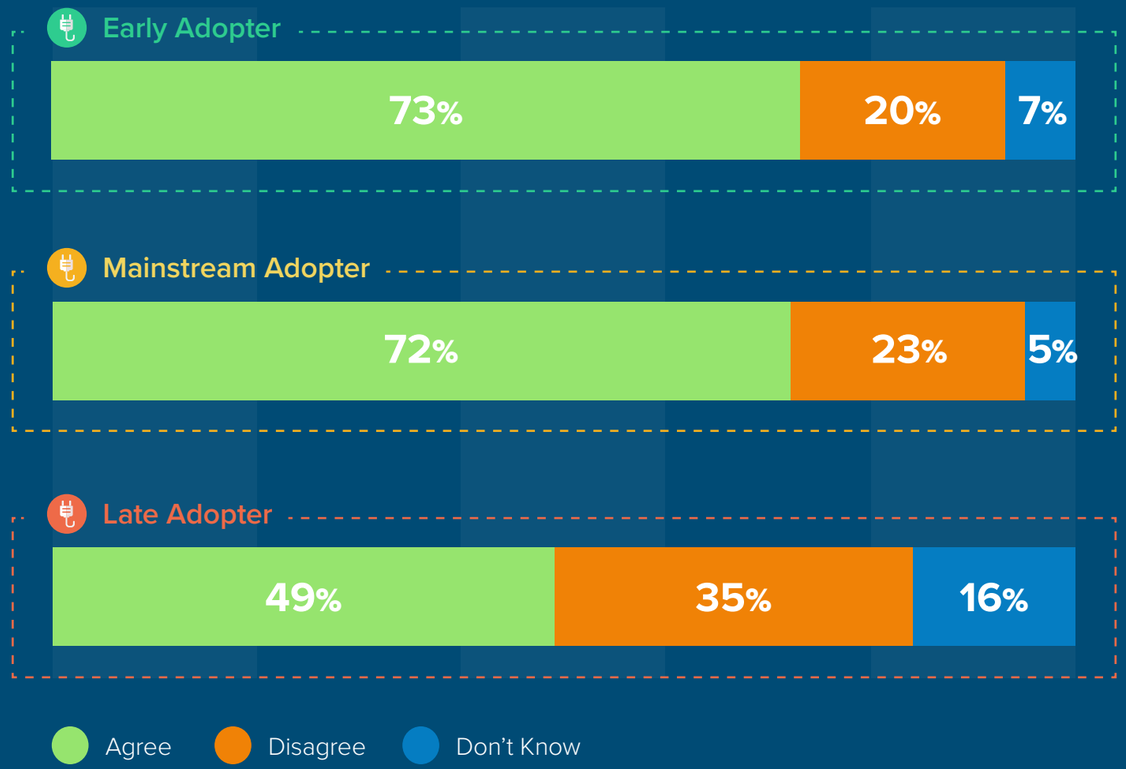
SUPPORT FOR IAM TOOLS: INTERNAL INFRASTRUCTURE

60% or more of state and local government respondents indicate that their organization has the IAM infrastructure to effectively manage access to internal applications and/or resources.



Q: "My organization has the IAM infrastructure to effectively manage access to internal applications / resources."

A higher percentage of late adopters say they don't have the necessary infrastructure.

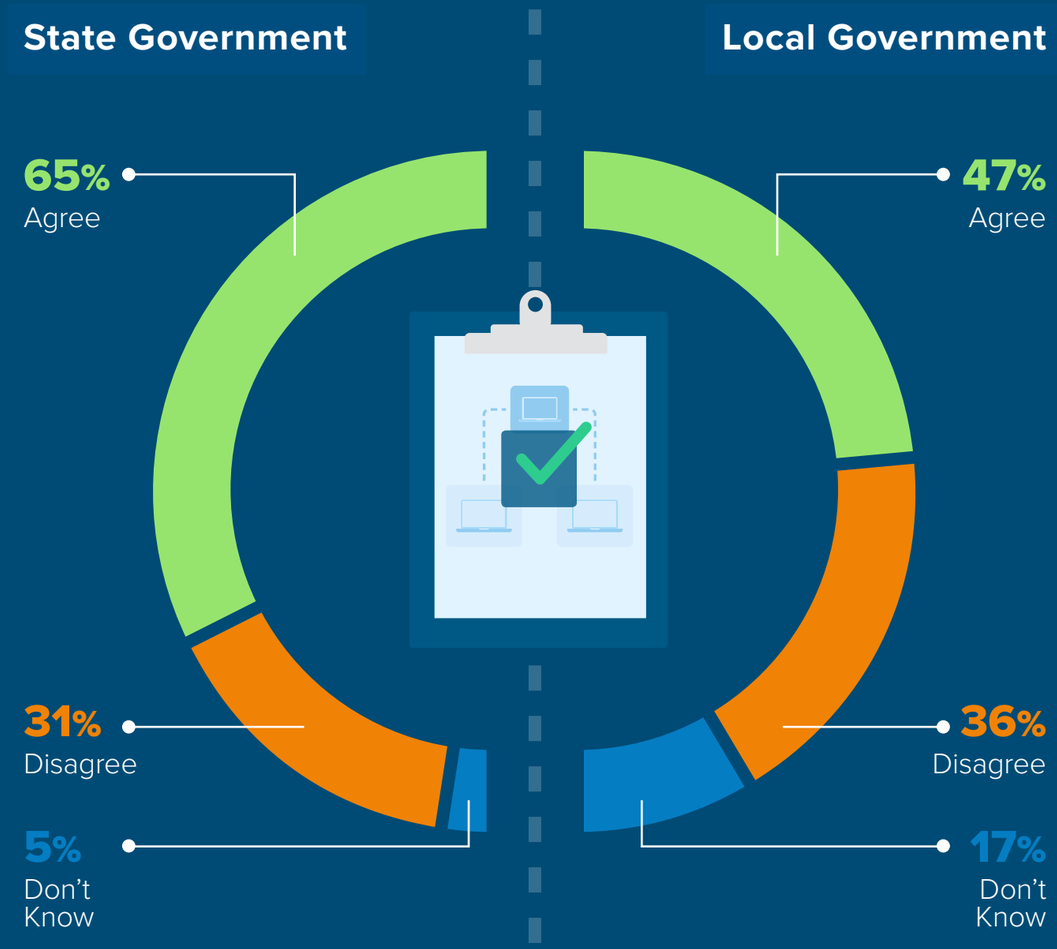


*Percentages don't add to 100% due to rounding

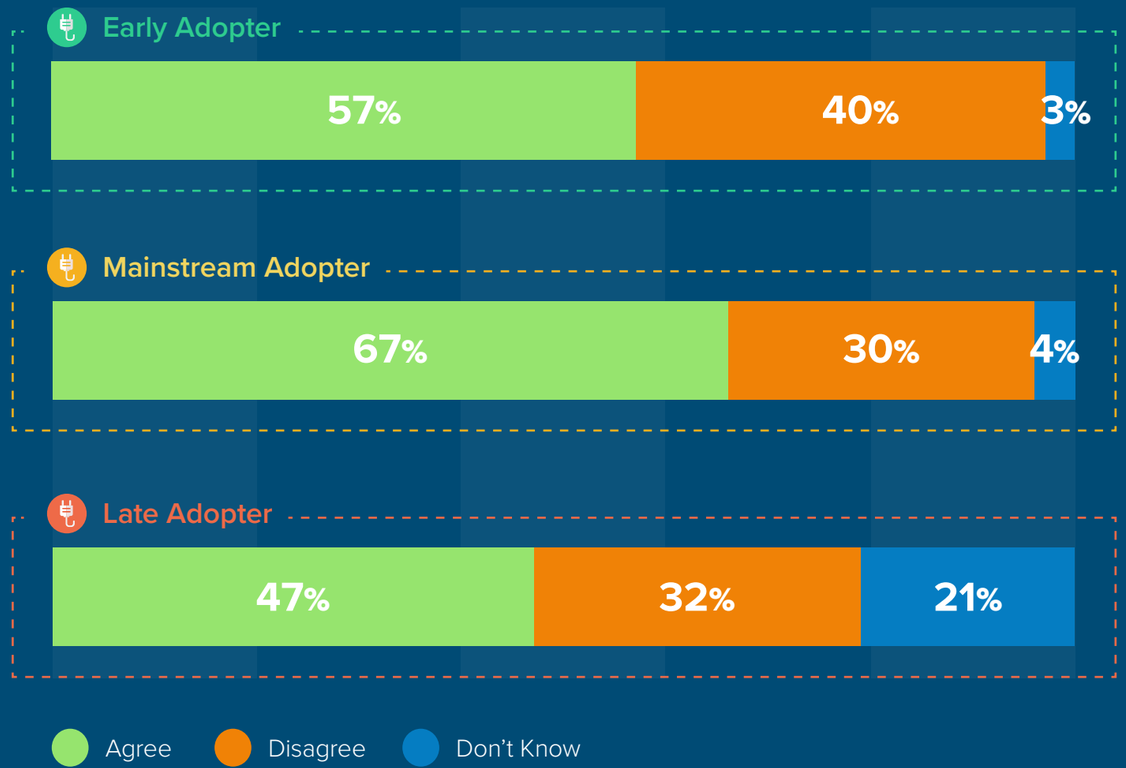
Take-away: *The unseen challenge is that most government infrastructure is currently not designed for modern systems or cloud applications. As agencies modernize its systems, more applications will require modern IAM tools.*

SUPPORT FOR IAM TOOLS: THIRD-PARTY APPLICATIONS

State agencies are further along than local agencies in having the infrastructure to manage **access to third-party applications.** However, one-third or more of respondents say they don't have the necessary infrastructure, suggesting key gaps in visibility into user access and the potential for significant security blind spots.



Mainstream adopters appear further along than early and late adopters in managing access to third-party applications.



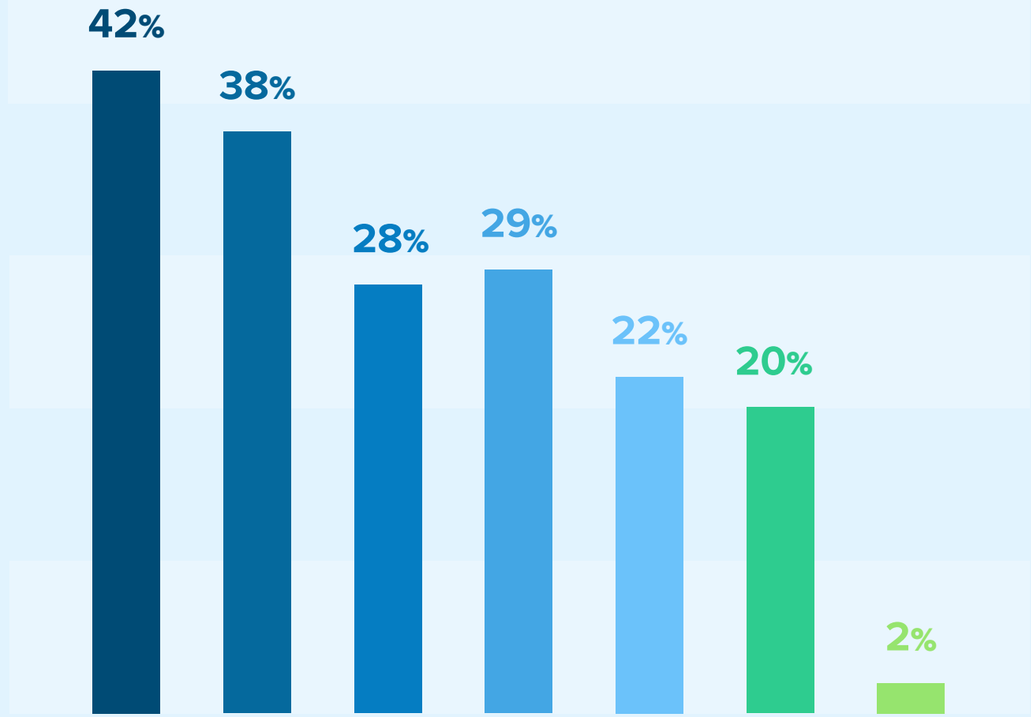
*Percentages don't add to 100% due to rounding

Q: "My organization has the IAM infrastructure to effectively manage access to *third-party* applications / resources."

CHALLENGES TO PURSUING IAM SOLUTIONS

Take-away: *Despite having management support, tools and resources, and an internal infrastructure to manage an IAM strategy, some agencies may not be able to elevate the implementation of IAM solutions to the top of their list of priorities, exposing them to increased risks...*

42% of respondents reported higher IT priorities and **38% stressed a lack of IT staff expertise** for top challenges to implementing IAM tools/services. In addition to the complexity of implementing IAM tools/services, agencies face many challenges that hold them back from implementing IAM more quickly.



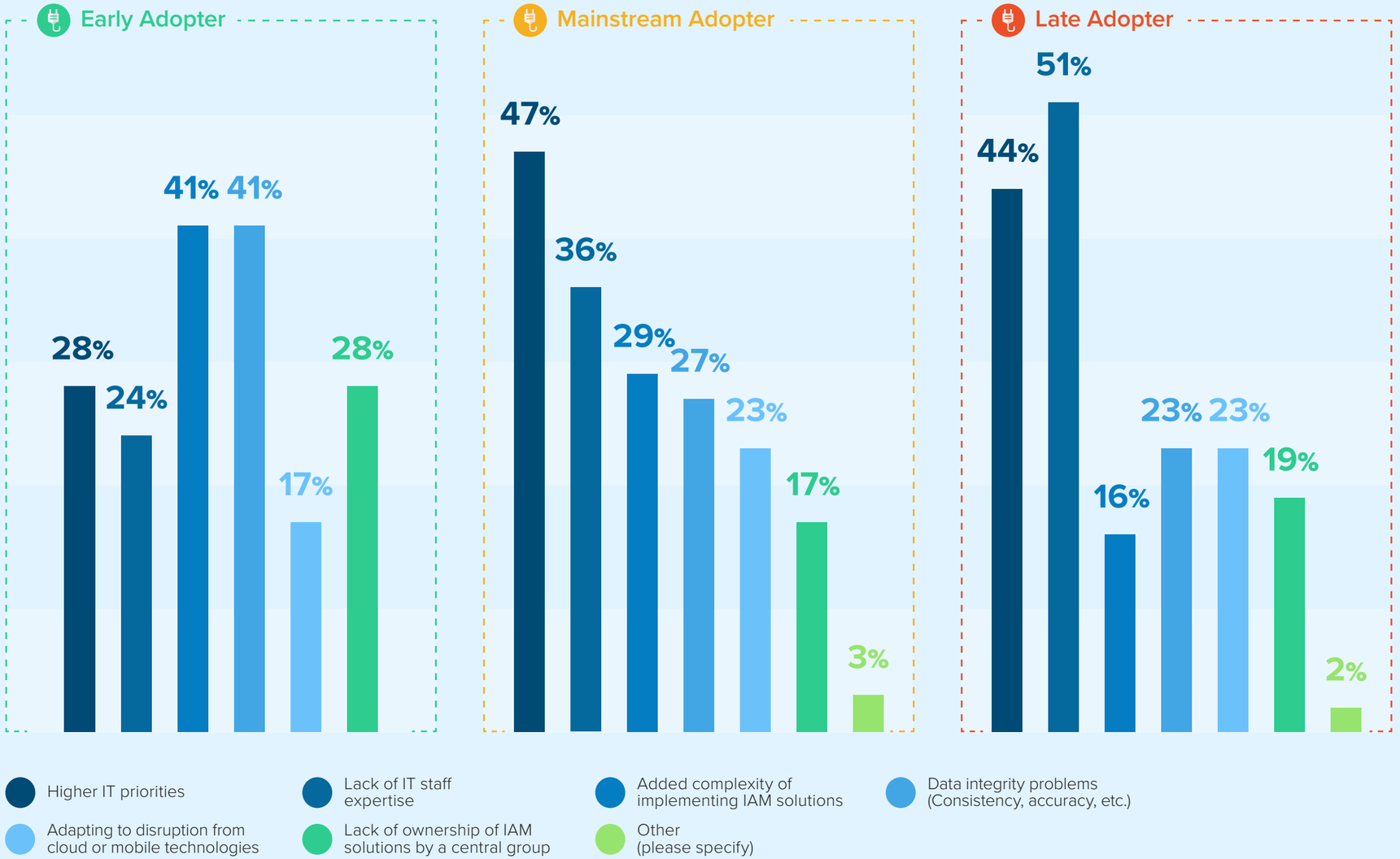
All Respondents – State and Local

- Higher IT priorities
- Lack of IT staff expertise
- Added complexity of implementing IAM solutions
- Data integrity problems (Consistency, accuracy, etc.)
- Adapting to disruption from cloud or mobile technologies
- Lack of ownership of IAM solutions by a central group
- Other (please specify)

Q: What other challenges does your organization face pursuing IAM solutions? (Select up to three)

CHALLENGES TO PURSUING IAM SOLUTIONS

Agencies that identify being at different states of technology adoption face different challenges. **Early adopters** tend to struggle more with the added **complexity of implementing IAM solutions and data integrity issues (41%)**. Mainstream adopters face greater challenges from **competing IT priorities (47%)**. Late adopters struggle most with a **lack of IT expertise (51%)**.



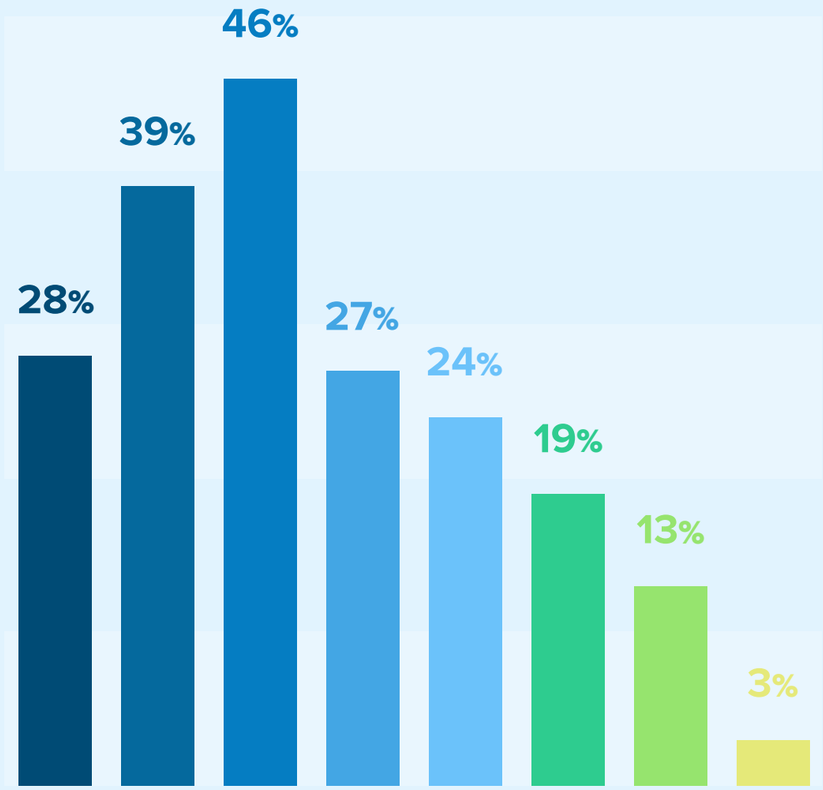
Q: What other challenges does your organization face pursuing IAM solutions? (Select up to three)

DRIVERS FOR IAM TOOLS/SERVICES ADOPTION

Security and privacy concerns are driving agency IT leaders most in adopting IAM tools and services, followed by opportunities to reduce costs, enhance services and user satisfaction.

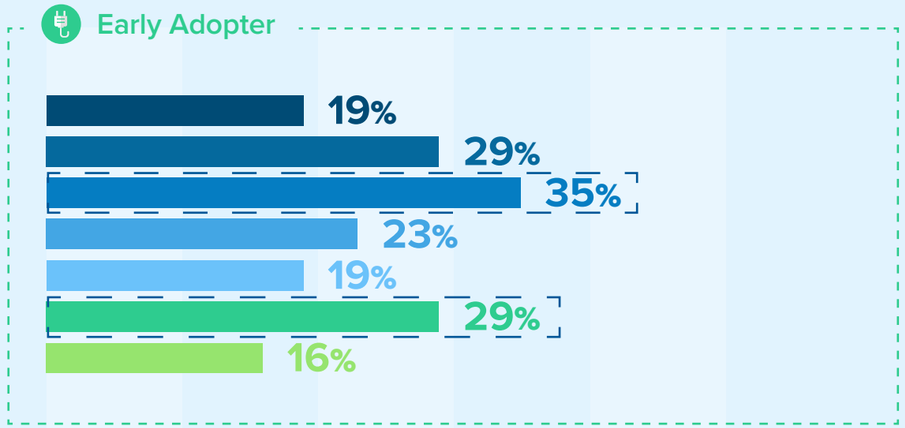
Early (35%) and mainstream (53%) adopters understand IAM's strategic value to reduce security risk. Additionally, early adopters (29%) report that IAM solutions make them less dependent on vendors.

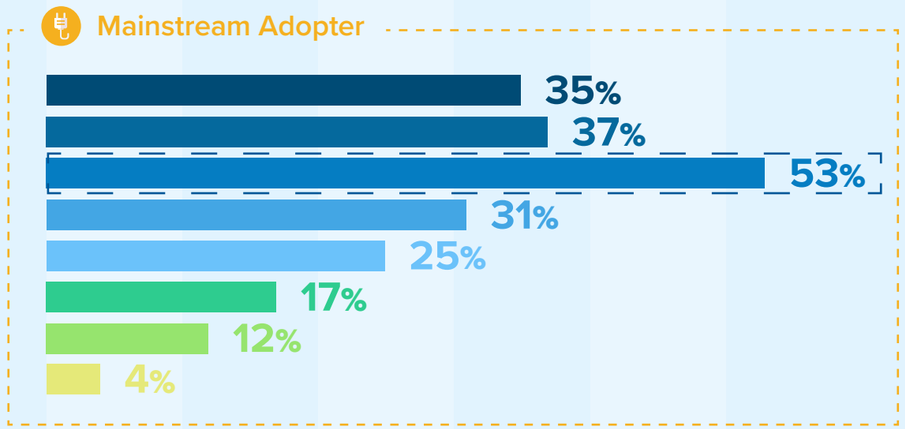
Take-away: IAM solutions appear to address a combination of IT issues. By managing IAM centrally, agencies can improve security and regulatory compliance, streamline costs and preserve agility by avoiding certain dependencies on vendors in controlling access privileges.

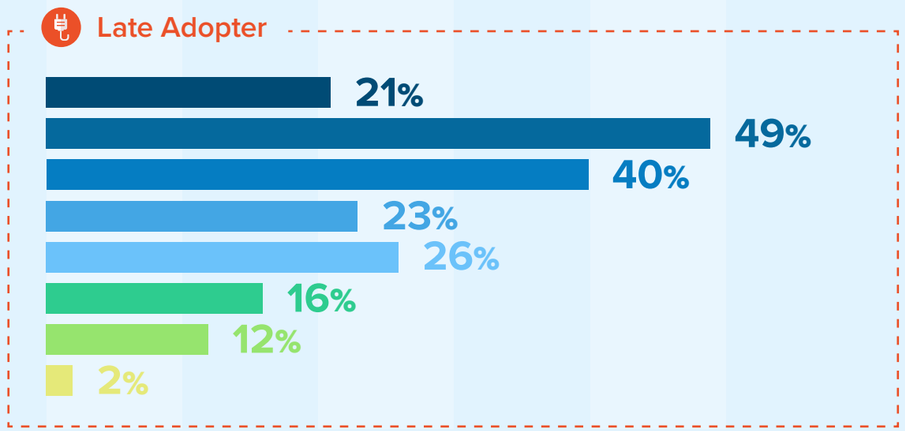


All Respondents – State and Local

- Enhanced user services and satisfaction
- Cost Reduction/ increased efficiencies
- Security/Privacy best practices
- Improvements in our technical environment
- Regulatory compliance (e.g., HIPAA, GLB Act, FERPA)
- Reduce vendor dependencies
- Strategic value/ opportunities
- Other (please specify)





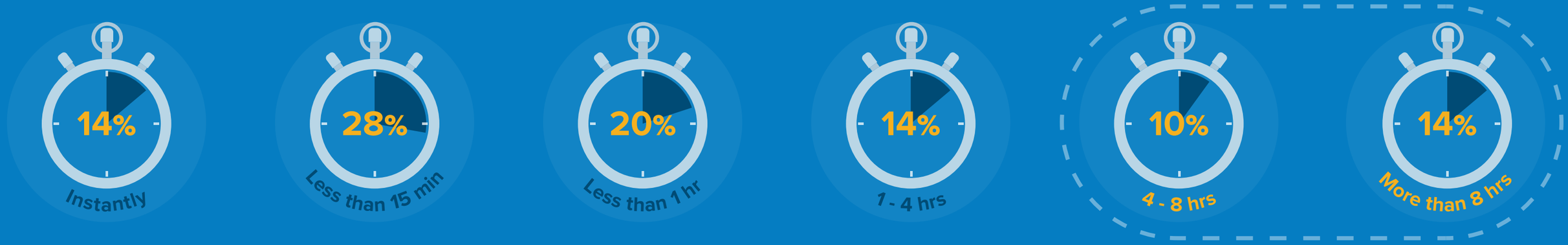


Q: What are the primary drivers for pursuing IAM tools/services at your organization? (Select up to three)

AUTHENTICATING NEW USERS

24% of respondents say it currently takes 4 hours or more to onboard new users, representing a loss of productivity for new employees.

Currently Takes



71% of respondents said authenticating and provisioning new users to access applications and services **should take less than 15 minutes**, compared to 42% of respondents who say they can accomplish that currently.

Should Take

**Percentages don't add to 100% due to rounding*

Take-away: *Extensive onboarding time negatively impacts efficiency across the agency, as well as employee experience and satisfaction.*

Q: How long does it take your organization to authenticate and fully provision a new user to access the applications and services they need? How long should it take?

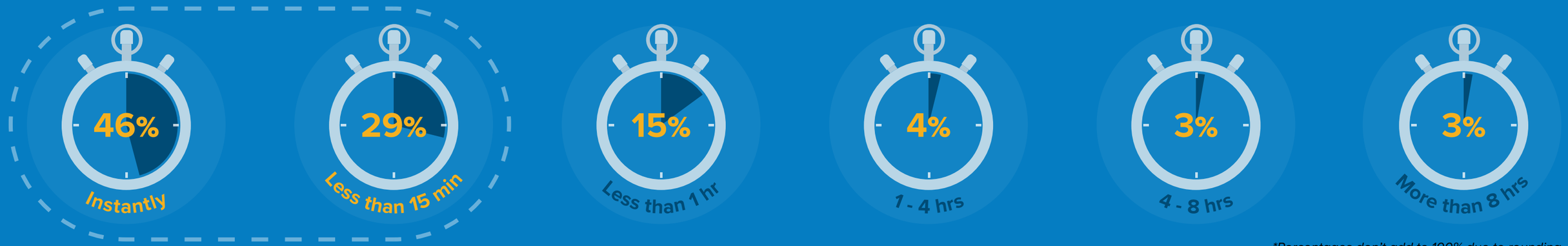
DISABLING USER ACCESS

1 in 6 respondents say it currently takes 4 hours or more to disable user access privileges, suggesting many state and local agencies face significant risks of data exfiltration by departing employees.

Currently Takes

75% of respondents indicated that disabling user access privileges **should take less than 15 minutes,** compared to 42% of respondents who say they can accomplish that currently.

Should Take



**Percentages don't add to 100% due to rounding*

Take-away: Revoking access of a former employee or contractor will limit risk of inappropriate access or breach of sensitive information.

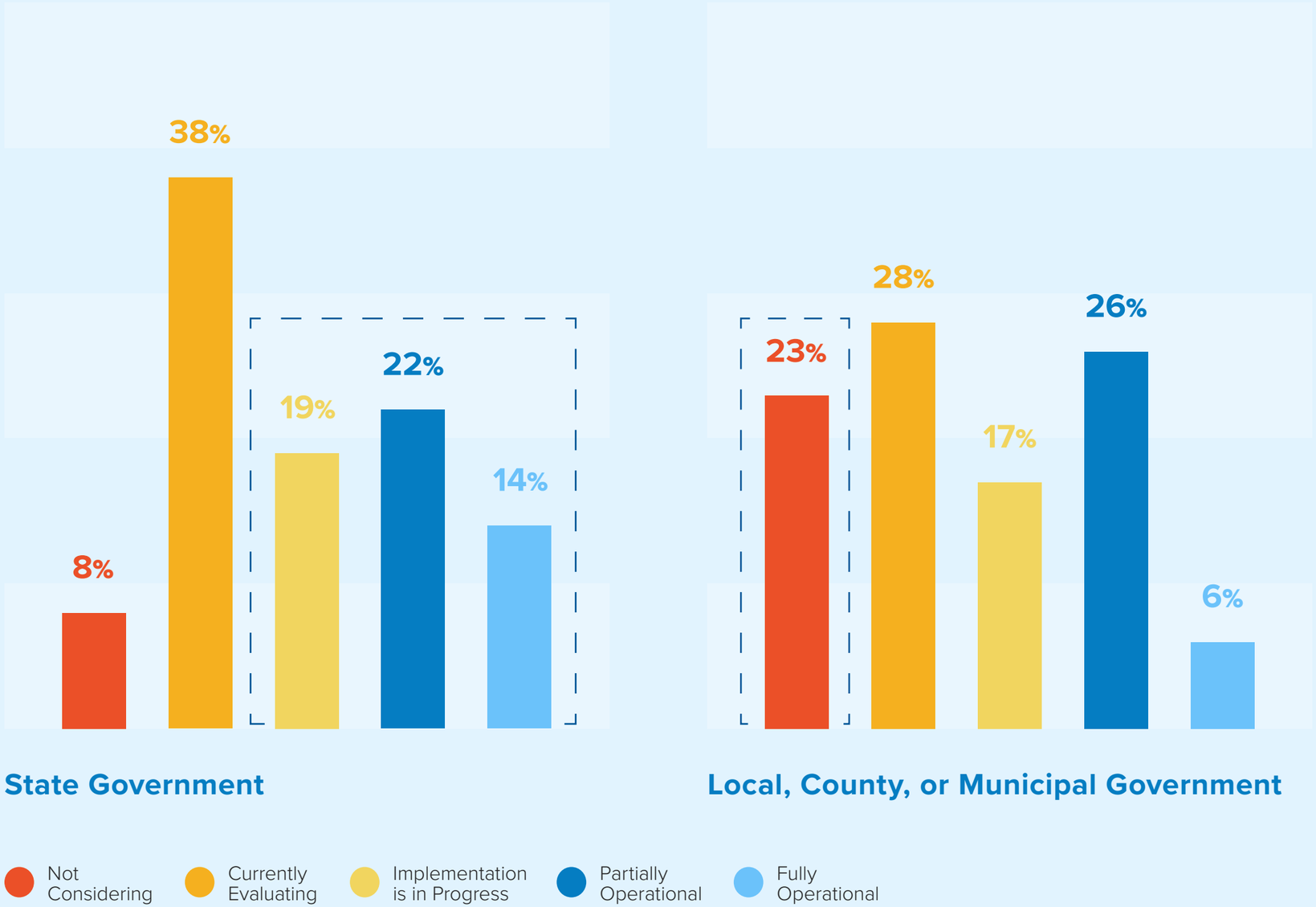
Q: How long does it take your organization to disable user access privileges once a user is no longer affiliated with your organization? How long do you believe it should take?

SINGLE SIGN-ON ADOPTION

55% of state government respondents are in some stage of implementing or operating a single sign-on approach to access internal and third-party applications. Another 38% are evaluating that approach.

This is contrasted by **23%, of local government** respondents who report they are still not considering it.

Take-away: *As agencies increase their number of applications, it increases its risk of users falling into poor password practices. Single sign-on would help mitigate those risks.*



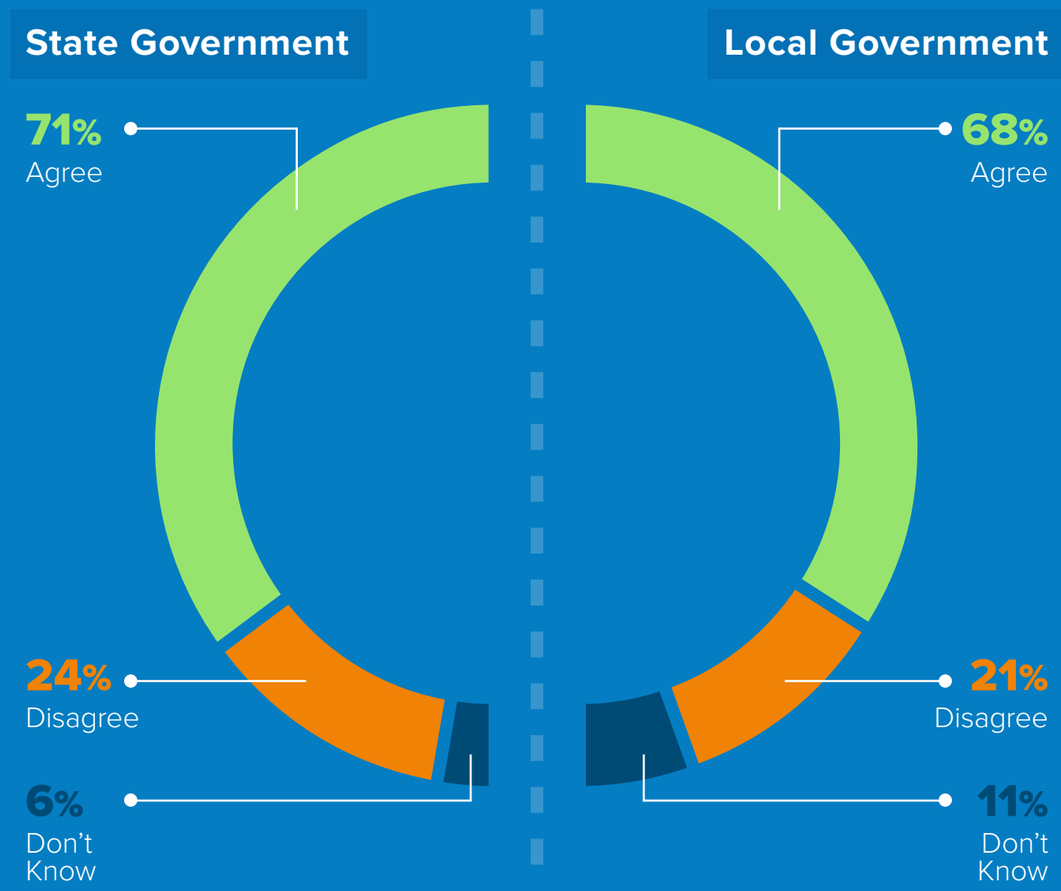
**Percentages don't add to 100% due to rounding*

Q: To what extent is your organization using or considering a single sign-on approach to access internal and third-party applications?

SUPPORT FOR MULTIFACTOR AUTHENTICATION

71% of state and 68% of local government respondents view multifactor authentication (MFA) as essential to effective IAM.

Requiring multiple factors to grant access to agency applications significantly improves the security posture of an IT environment. The findings suggest strong support of MFA across both state and local government agencies as a method to improve security.



**Percentages don't add to 100% due to rounding*

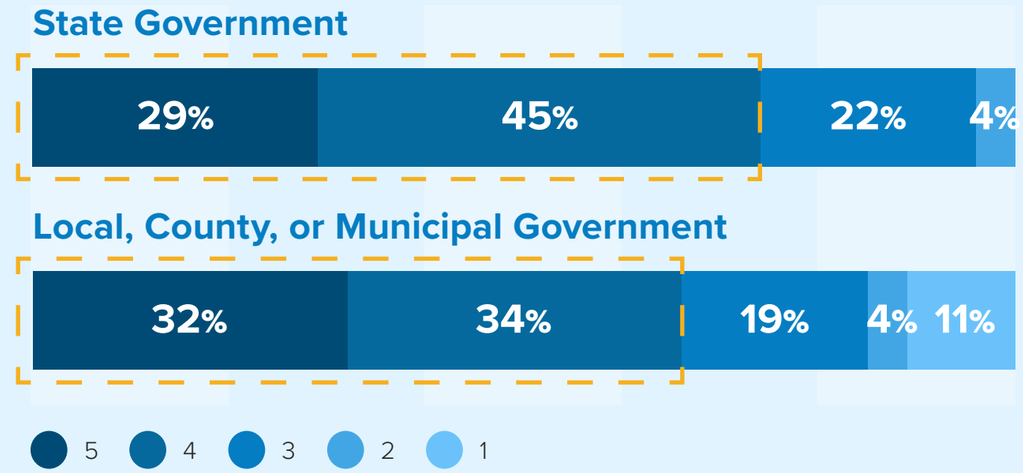
Q: "Multifactor authentication is essential to effective identity and access management."

CENTRALIZED VIEW OF ENTERPRISE DIRECTORY

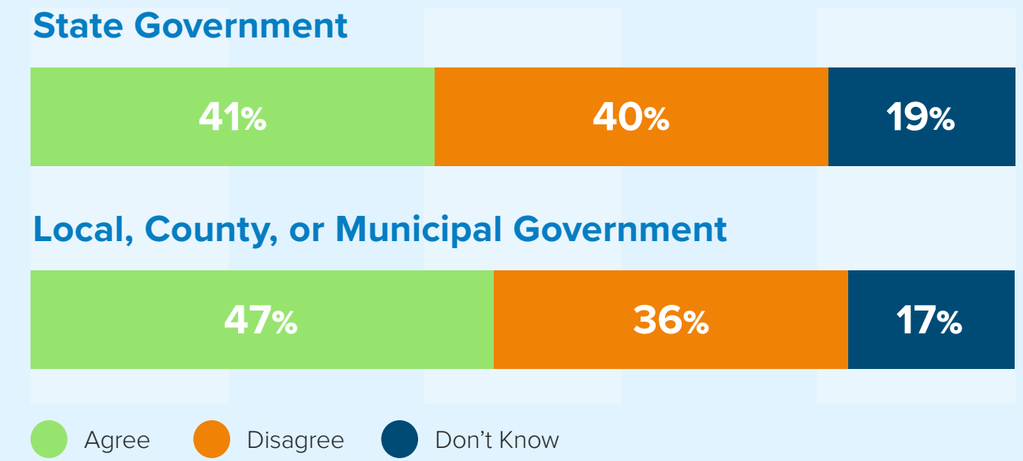
Three-fourths of state and **two-thirds** of local government respondents said having a centralized view of the enterprise directory is important for network and application security/efficiency — far more than actually have it.

41% of state and **47% of local government** respondents reported that their agencies have a centralized view of their enterprise directory.

Take-away: That gap suggests state and local government leaders are open to solutions that would help them achieve a centralized view of enterprise directories.



Q: How important is it to have a centralized view of your enterprise directory(ies) for network and application security/efficiency? (On a scale where 5 = high, 1 = low)



Q: Do you have a centralized view of your enterprise directory(ies)?

CONCLUSIONS

The state of IAM tools in state and local government

- Security concerns are the number one factor driving the adoption of identity and access management tools and services, with 6 in 10 local government respondents and 7 in 10 state respondents who indicated automating IAM solutions is essential to addressing their agency's IT security concerns.

- While IAM solutions are seen as a way to lower IT support costs, they are also seen as a key factor in streamlining the user experience. That's likely to become more important in the coming year: Among state and local officials considered mainstream technology adopters, 59% anticipated supporting a greater number of applications for employees — and 45% anticipated a rise in public-facing applications used by citizens.

- Two-thirds of respondents also say automating IAM tools and services will be essential to efforts to adopt cloud computing services.

- Government agencies, however, have a ways to go: Only 28% of state respondents and 15% of local respondents reported having IAM tools fully or partially operational.

- Respondents said it takes longer to activate and deactivate user access privileges than they'd prefer. The findings suggest agencies face a continuing loss of productivity when onboarding new employees and risks of data exfiltration when employees leave.

- State and local agency IT officials also voiced significant support for solutions that provide users single sign-on capability, two-factor authorization and a centralized view of enterprise directories to manage access privileges.

NEXT STEPS

Five steps to better secure agency IT environments and offer a more seamless user experience:

1. **Select a solution built for the cloud –** IAM solutions designed for legacy on-premises applications were not built for the cloud and require custom integrations to make them work with modern solutions. Ensure every user is secure with pre-configured integrations and a directory of on premises cloud and mobile data access. This will eliminate the challenge of rebuilding custom integrations with every application update from the independent software vendor.

2. **Centralize identity –** Reduce password management risk by centralizing identity with a single sign-on solution and encourage better password practices from users.

3. **Enable strong authentication –** Passwords have inherent limitations, but multi-factor authentication methods strengthen identity assurance. Apply methods such as one-time passwords, soft or physical tokens, biometrics and manage policies for all applications so data is protected no matter where or how it is accessed.

4. **Reduce the attack surface –** Not knowing what data users have access to, especially as employees change or leave roles, can leave organizations with security blind spots. Simplifying the provisioning and deprovisioning of user access, and improving lifecycle management practices, eliminates blind spots and reduces possible entry points for attackers.

5. **Enable visibility and response –** Security shouldn't be restricted to silos. Centralizing identity enables a modern perimeter which provides greater visibility into seemingly disparate events. It also allows IT departments to identify and respond to possible threats faster.

statescoop

StateScoop is the leading media brand in the state and local government market. With more than 100,000 unique monthly visitors and 125,000 daily newsletter subscribers, StateScoop reports on news and events impacting technology decisions in state and local government. With our website, daily newsletter and events, we bring together IT leaders and innovators from across government, academia and industry to exchange best practices and identify ways to improve state and city government.

CONTACT:

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

PRESENTED BY statescoop

UNDERWRITTEN BY okta