

# SolarWinds Public Sector Cybersecurity Survey Report

November 2021



# Methodology

SolarWinds contracted Market Connections to design and conduct an online survey among 200 federal, 100 state and local, and 100 education decision-makers and influencers in October 2021. SolarWinds was not revealed as the survey sponsor.

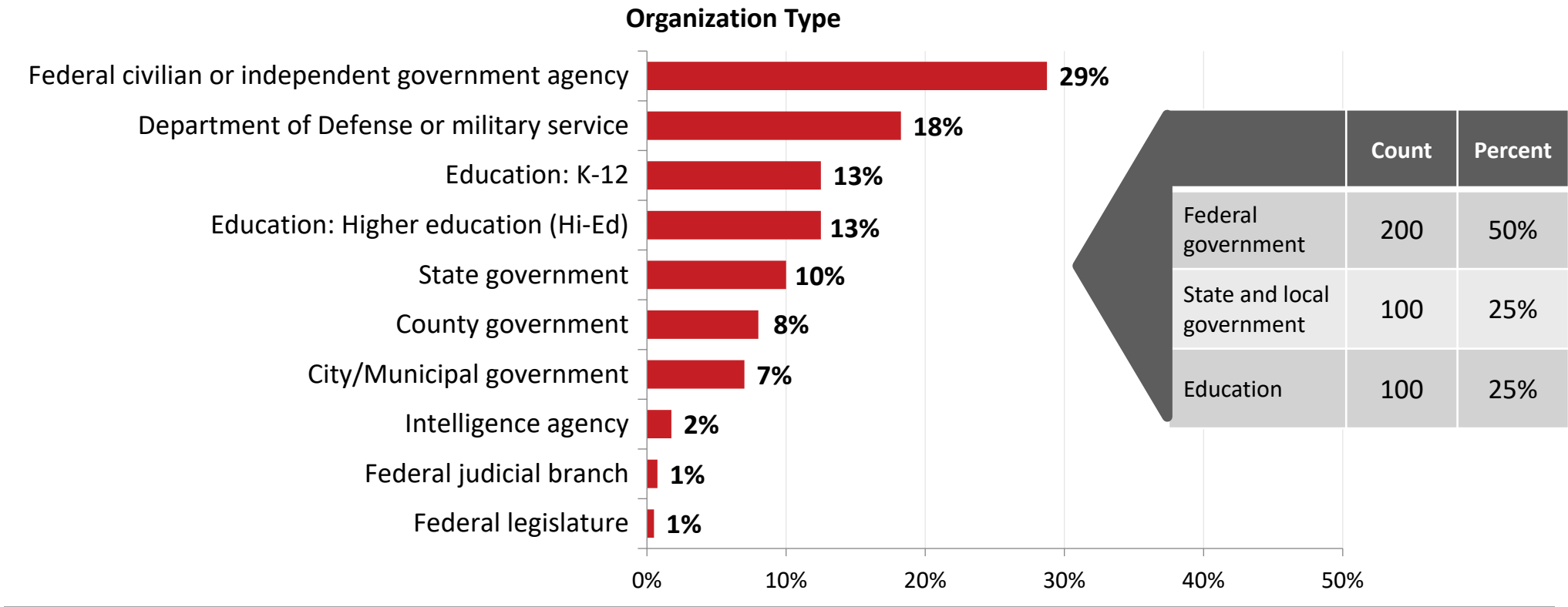



## PRIMARY OBJECTIVES:

- Determine challenges faced by public sector IT professionals and sources of IT security threats
- Evaluate the importance of IT security products, solutions, and services and rate investment priorities
- Determine familiarity with the White House Cyber Security Executive Order and the perceived impact of its objectives
- Identify if organizations are using a zero-trust approach to IT, their motivations and deterrents, and evaluate the Principle of Least Privilege (PoLP)
- Measure the use of teleworking before COVID-19, currently, and in the future

# Organizations Represented

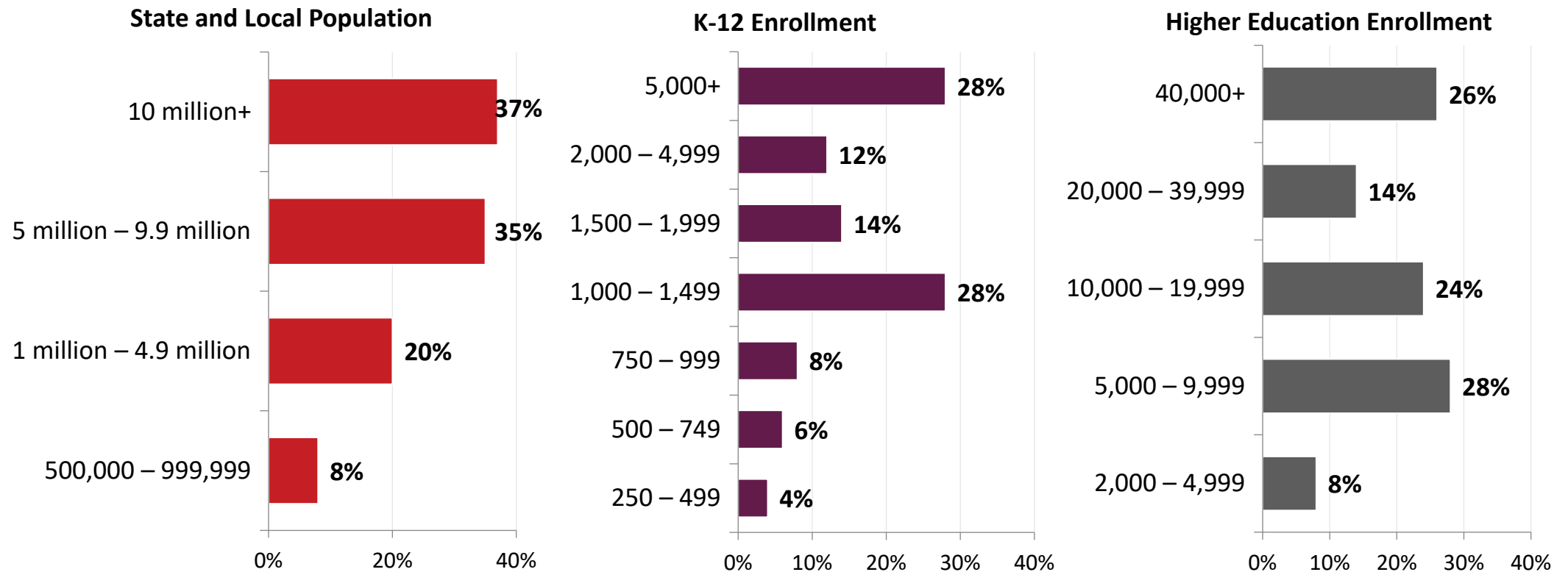
All respondents work for the public sector with half in the federal government, one-quarter in state and local government, and one-quarter in education.



 Which of the following best describes your current employer?

# SLED Population and Enrollment

A range of state and local populations and school enrollments are represented in the sample. Smaller state, local, and education (SLED) populations and enrollments were excluded from participating.



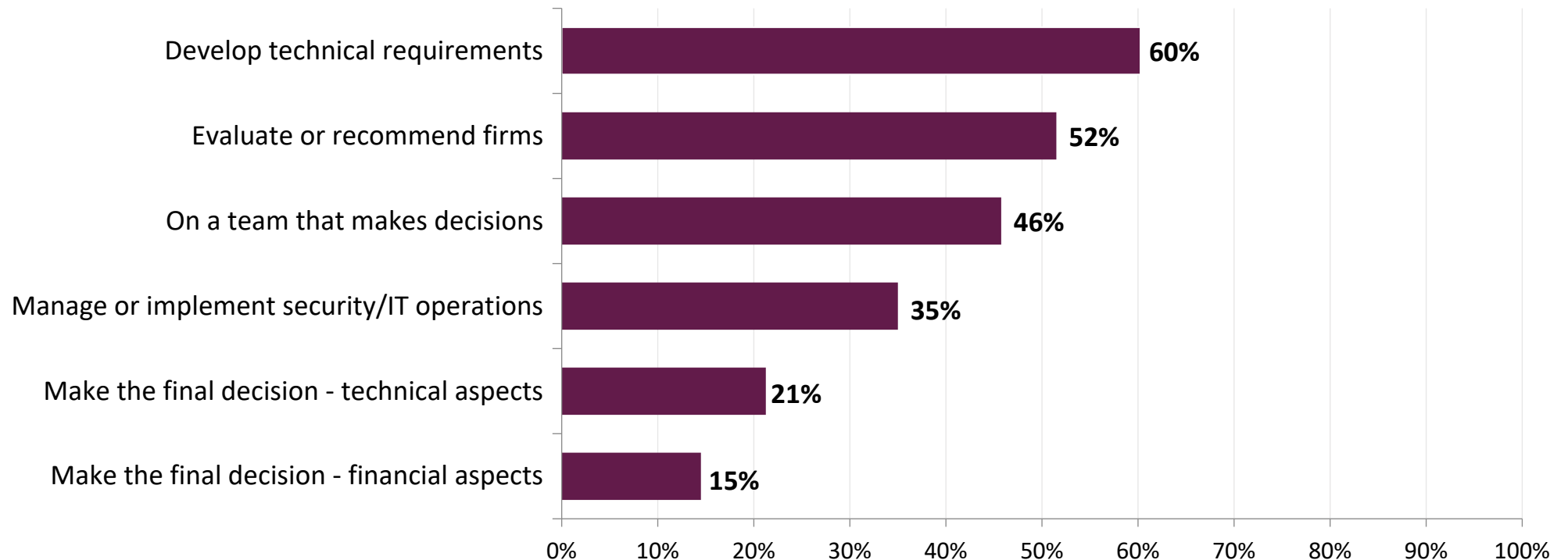
[STATE, COUNTY, OR CITY GOVERNMENT] What is the estimated population of the ["state," "county," OR "city"] that you work for?

[EDUCATION: K-12] How many total students are currently enrolled at the school(s) where you are involved with IT security and/or IT operations and management?

[EDUCATION: HIGHER EDUCATION] How many students are currently enrolled at your college or university?

# Decision-Making Involvement

All respondents are knowledgeable or involved in decisions and recommendations regarding IT operations and management and IT security solutions and services.



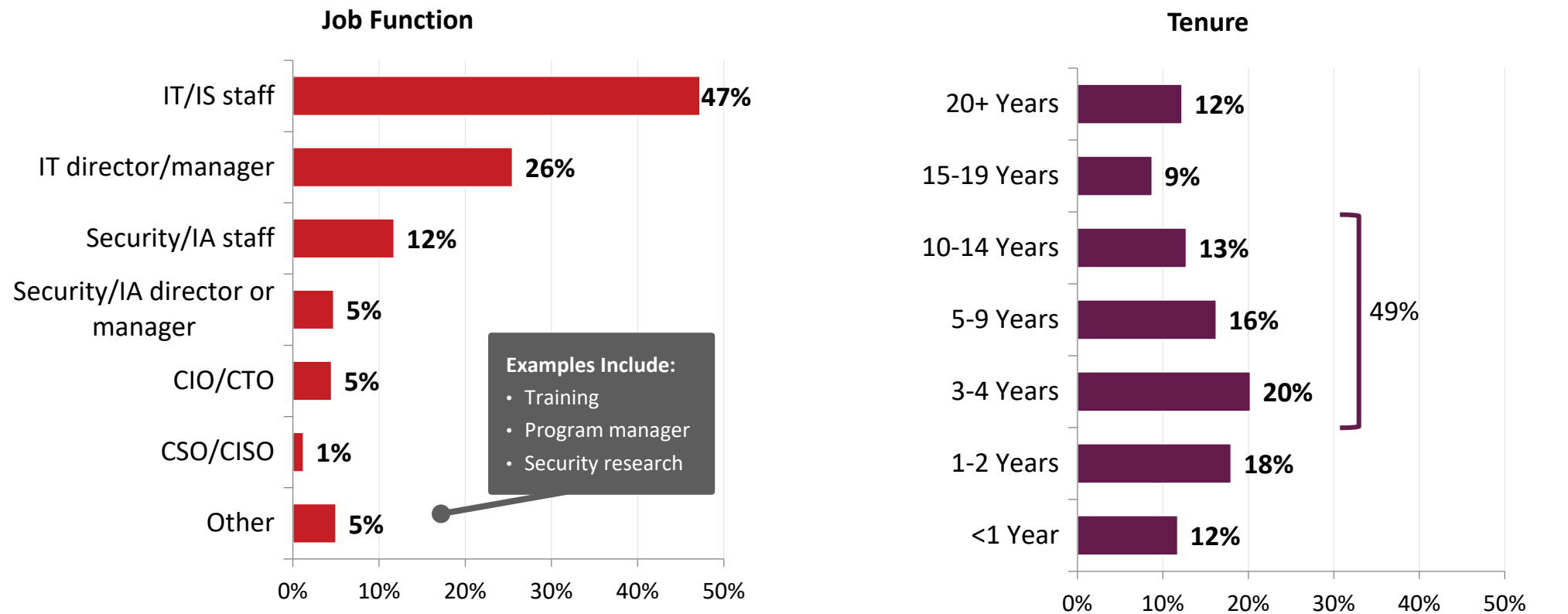
Note: Multiple responses allowed




How are you involved in your organization's decisions or recommendations regarding IT operations and management and IT security solutions and services? (select all that apply)

# Job Function and Tenure

A variety of job functions and tenures are represented in the sample, with most being IT staff and working at their current organization for 3-4 years, approximately half have a tenure of 3-14 years.

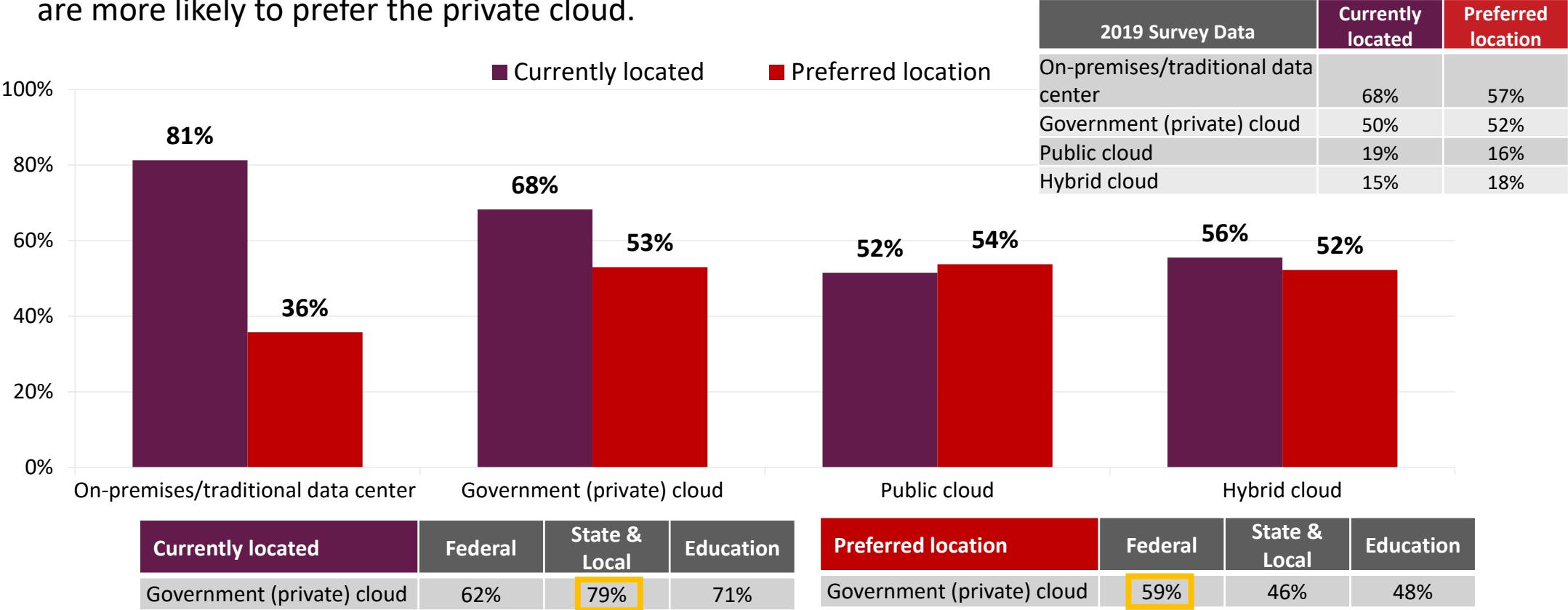


 Which of the following best describes your current job title/function? How long have you been working at your current organization?





# Location of IT Security Products

IT security products are located primarily on-premises or in a private cloud. The respondents' preferred location of these products is in some type of cloud, not on-premises. Federal respondents are more likely to prefer the private cloud.



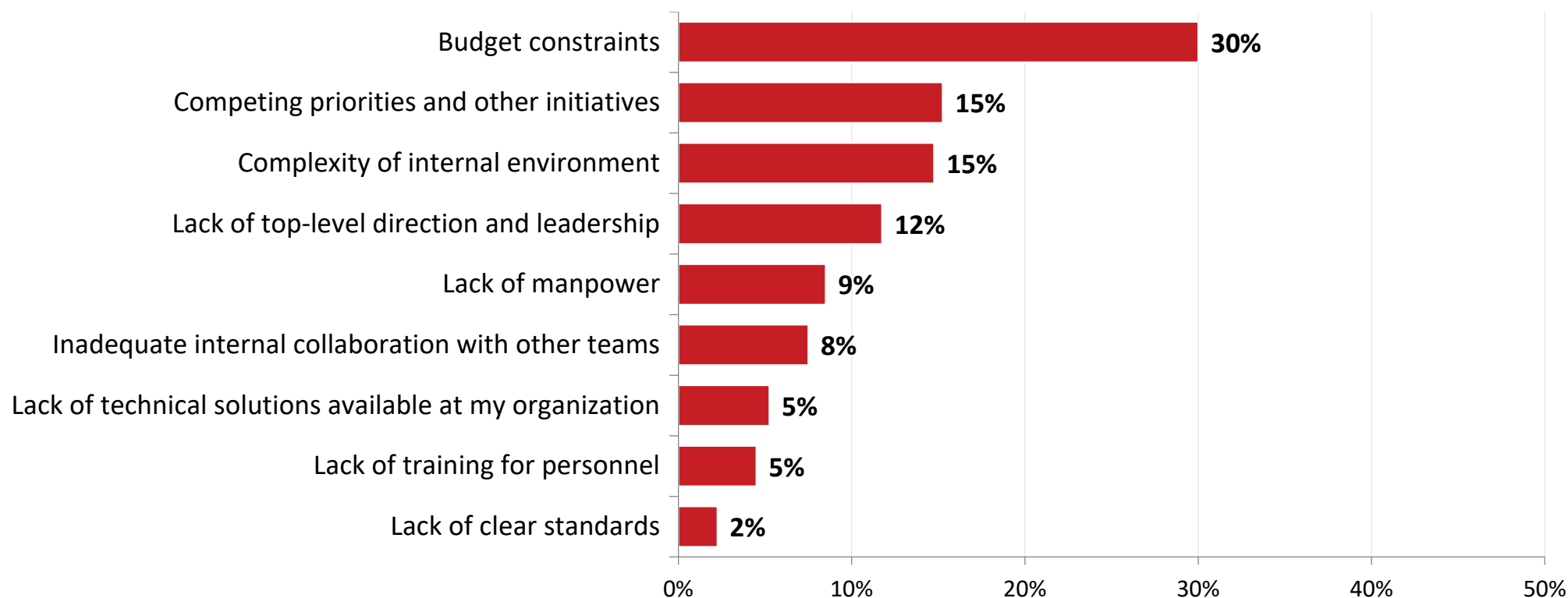
Note: Multiple responses allowed

 = statistically significant difference

 Where are the IT security products your organization uses currently? Where would you prefer these products to be located? (select all that apply)

# IT Security Obstacles

Budget constraints top the list of significant obstacles to maintaining or improving organization IT security. Competing priorities and a complex internal environment also impact IT security improvement.



What is the most significant high-level obstacle to maintaining or improving IT security at your organization?




# IT Security Obstacles by Organization Type

- Education respondents cite lack of top-level direction and leadership as an obstacle more than other public sector respondents.
- State government respondents indicate more so than local governments that budget constraints are an obstacle to maintaining or improving IT security.

	Federal	State & Local	Education
Budget constraints	30%	35%	26%
Competing priorities, other initiatives	14%	14%	19%
Complexity of internal environment	18%	12%	12%
Lack of top-level direction and leadership	8%	13%	18%

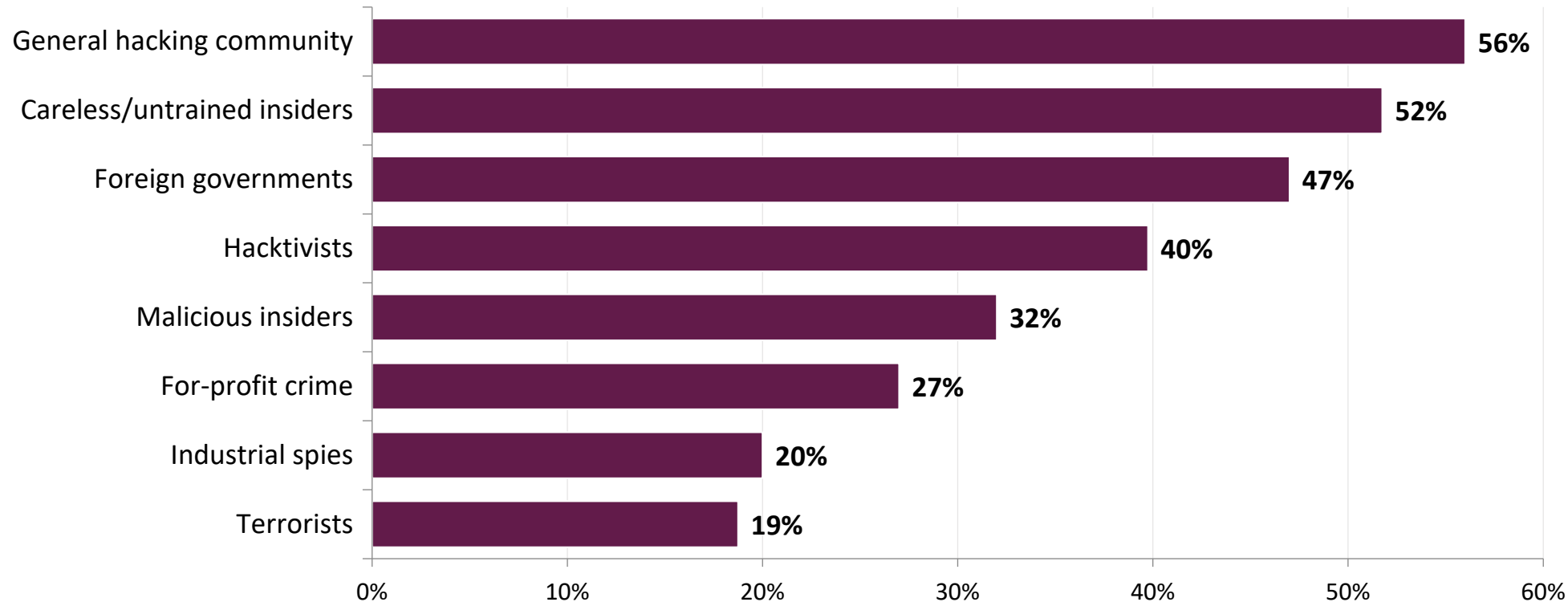
State & Local Gov	State	Local
Budget constraints	50%	25%

 = statistically significant difference

What is the most significant high-level obstacle to maintaining or improving IT security at your organization?

# Sources of Security Threats

The general hacking community is the largest source of security threats at public sector organizations, followed closely by careless/untrained insiders.



Note: Multiple responses allowed




What are the greatest sources of IT security threats to your organization? (select all that apply)


# Sources of Security Threats by Organization Type

- State and local governments are significantly more likely than other public sector groups to mark the threat of the general hacking community (the top source of threats overall).
- Federal civilian agency respondents are more likely to indicate the general hacking community and careless insiders as a threat compared to defense.
- Significantly more federal respondents than education organizations indicate foreign governments and terrorists as threats. Defense respondents are more likely to note foreign governments.

	Federal	State & Local	Education	Defense	Civilian
General hacking community	56%	63%	49%	46%	63%
Careless/untrained insiders	52%	51%	53%	41%	58%
Foreign governments	59%	46%	25%	68%	53%
Terrorists	23%	18%	11%	25%	22%

Note: Multiple responses allowed

 = statistically significant difference


 What are the greatest sources of IT security threats to your organization? (select all that apply)


# Sources of Security Threats – Federal Trend

The top three sources of security threats have remained the same for the federal audience since 2014. There are significant increases from 2019 to 2021 for threats from foreign governments, the general hacking community, and hacktivists.

Federal	2014	2015	2016	2017	2018	2019	2021
Foreign governments	34%	38%	48%	48%	52%	48%	59%
General hacking community	47%	46%	46%	38%	48%	40%	56%
Careless/untrained insiders	42%	53%	48%	54%	56%	52%	52%
Hacktivists	26%	30%	38%	34%	31%	26%	42%
Malicious insiders	17%	23%	22%	29%	36%	29%	30%
For-profit crime	11%	14%	18%	17%	15%	20%	27%
Terrorists	21%	18%	24%	20%	25%	22%	23%
Industrial spies	6%	10%	16%	12%	19%	16%	23%

Note: Multiple responses allowed

 = statistically significant difference 2019-2020  = top three sources

 What are the greatest sources of IT security threats to your organization? (select all that apply)

# Sources of Security Threats – State/Local + Education

The top three sources of security threats have remained the same for the SLED audience since 2019.


State/Local	2019	2021
General hacking community	40%	63%
Careless/untrained insiders	52%	51%
Foreign governments	48%	46%
Hacktivists	26%	43%
Malicious insiders	29%	36%
For-profit crime	20%	29%
Industrial spies	16%	21%
Terrorists	22%	18%


Education	2019	2021
Careless/untrained insiders	52%	53%
General hacking community	40%	49%
Malicious insiders	29%	33%
Hacktivists	26%	32%
Foreign governments	48%	25%
For-profit crime	20%	25%
Industrial spies	16%	14%
Terrorists	22%	11%

Note: Multiple responses allowed



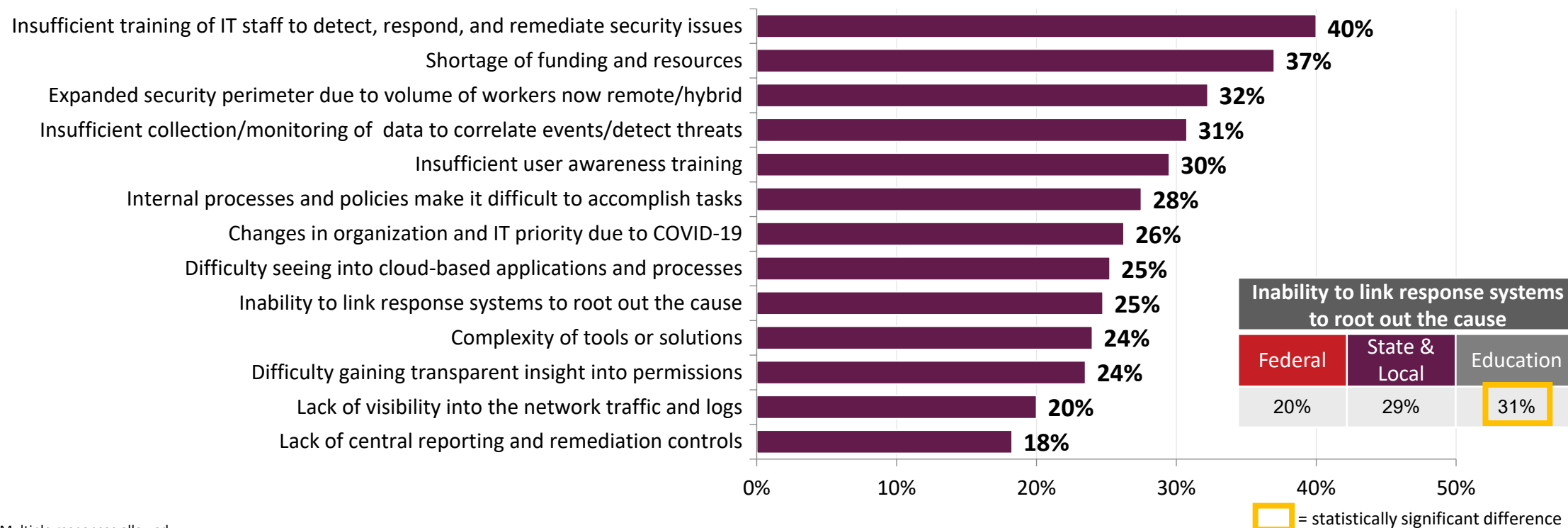
What are the greatest sources of IT security threats to your organization? (select all that apply)

 = statistically significant difference

 = top three sources

# Impediments to Detection/Remediation of Security Issues

The top impediments to detection/remediation are insufficient training of IT staff and shortage of funding and resources. Lack of visibility into network traffic/logs or lack of central reporting and remediation are less of an issue.



Note: Multiple responses allowed

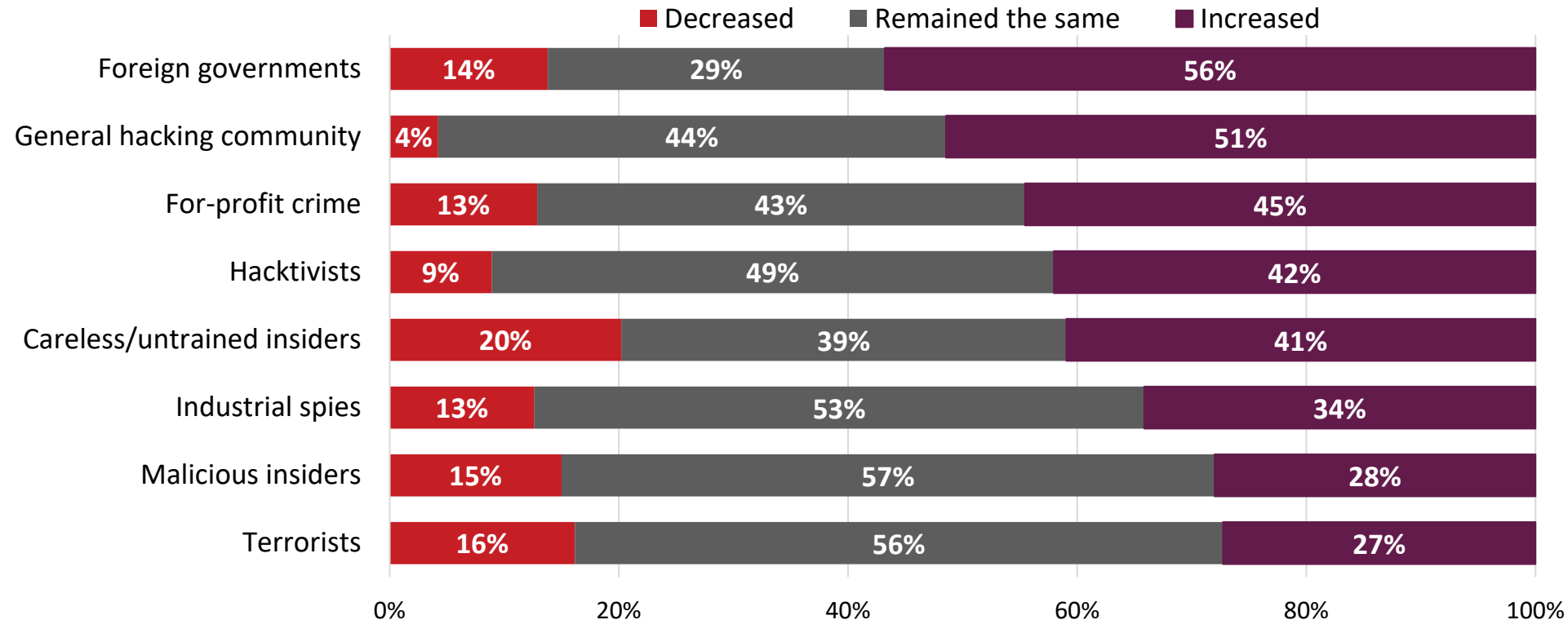


Which of the following are the greatest impediments to detection and remediation of security issues at your organization?



# Concern About IT Security Threats Since 2020

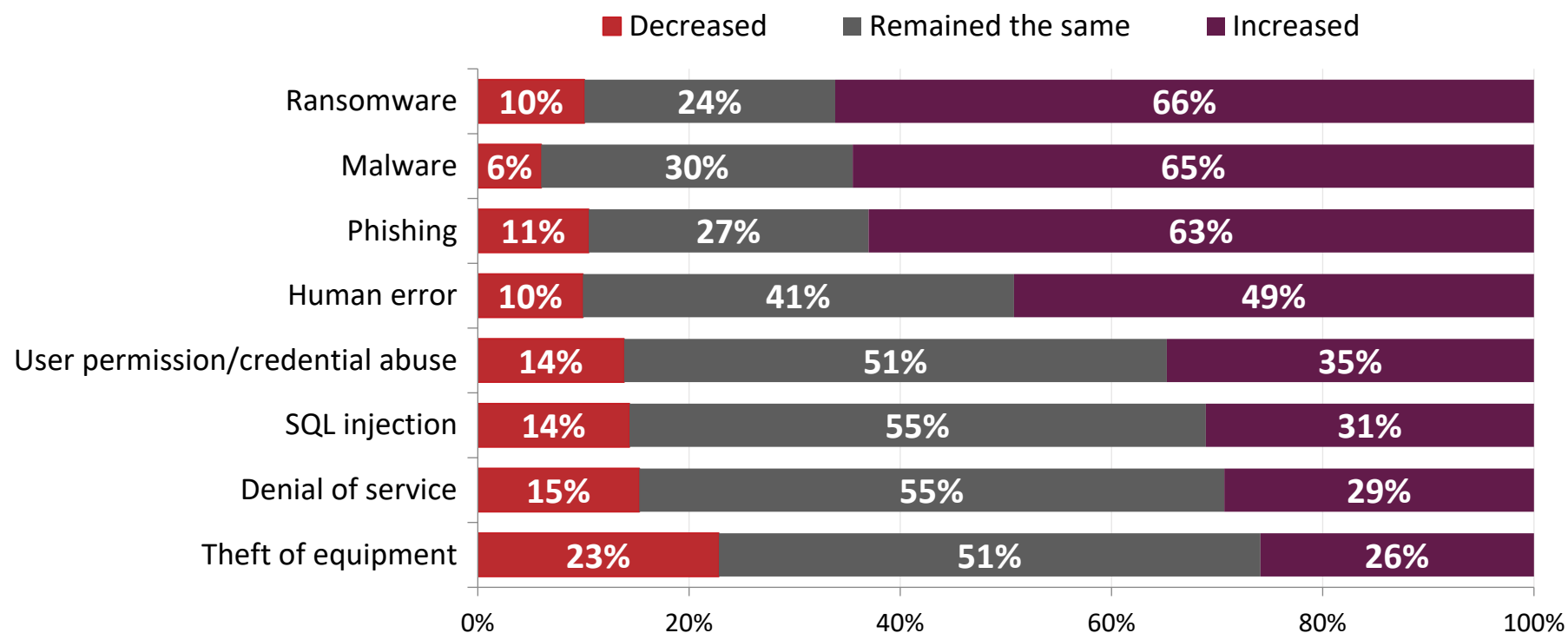
Increasing concerns about foreign governments and the general hacking community are the largest sources of security threats at public sector organizations.




Compared to 2020, has your level of concern changed regarding the following sources of IT security threats?

# Concern About Security Breaches Since 2020

Increasing concerns about security breaches with ransomware, malware, and phishing top the list for public sector organizations.



Decreased	Federal	State & Local	Education
Phishing	6%	20%	10%
Denial of Service	12%	22%	15%
Theft of equipment	25%	24%	15%

 = statistically significant difference

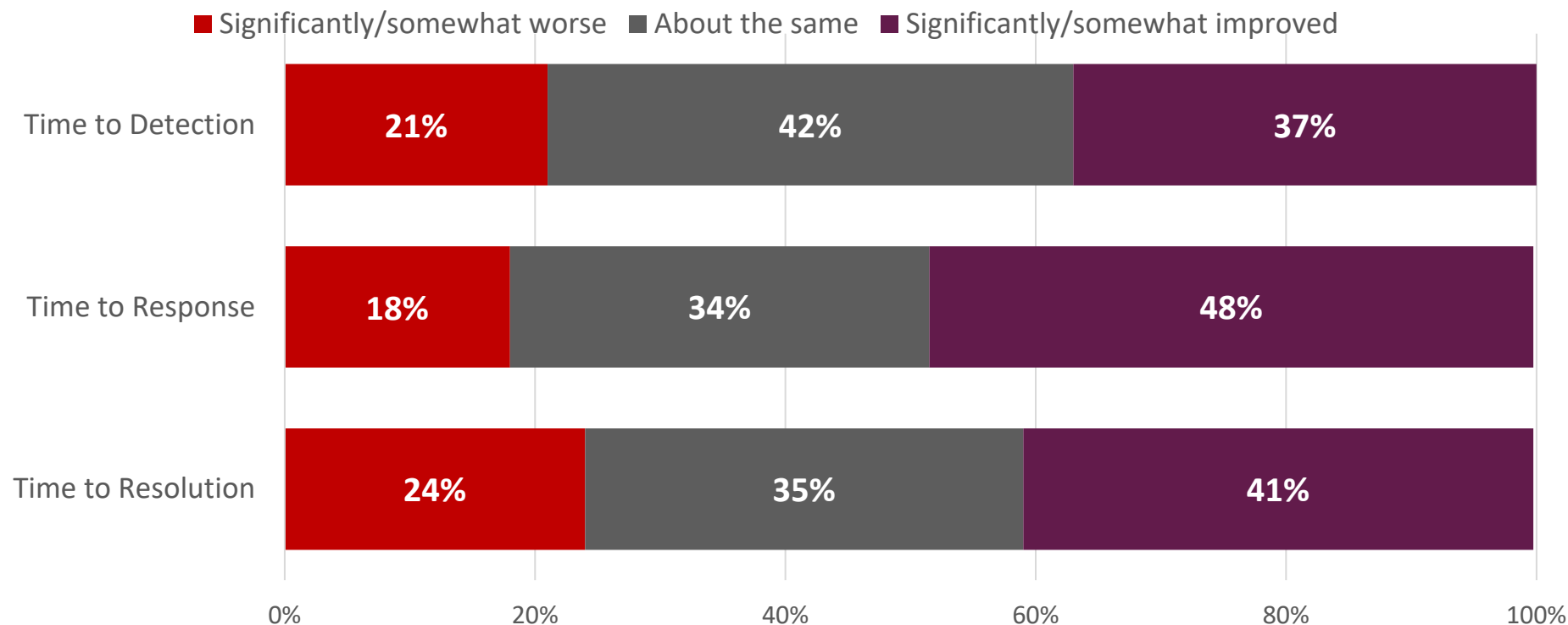
Note: Multiple responses allowed



Compared to 2020, has your level of concern changed regarding the following types of security breaches in 2021?

# Security Incidents and Events Since 2020

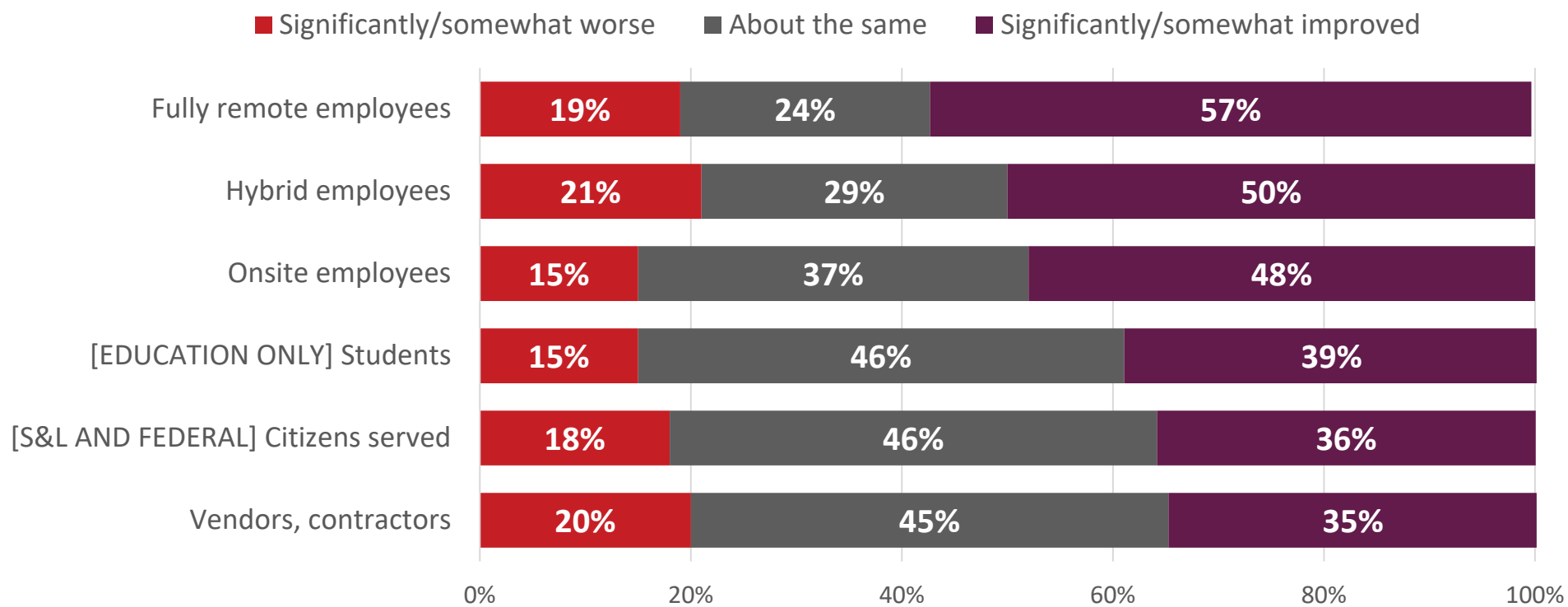
Approximately 6 out of 10 reported that time to detection and time to resolution has largely remained the same or worsened in 2021.



Compared to 2020 overall, how did each of the following change in your organization in 2021 regarding security incidents and events?

# Overall Security Posture Since 2020

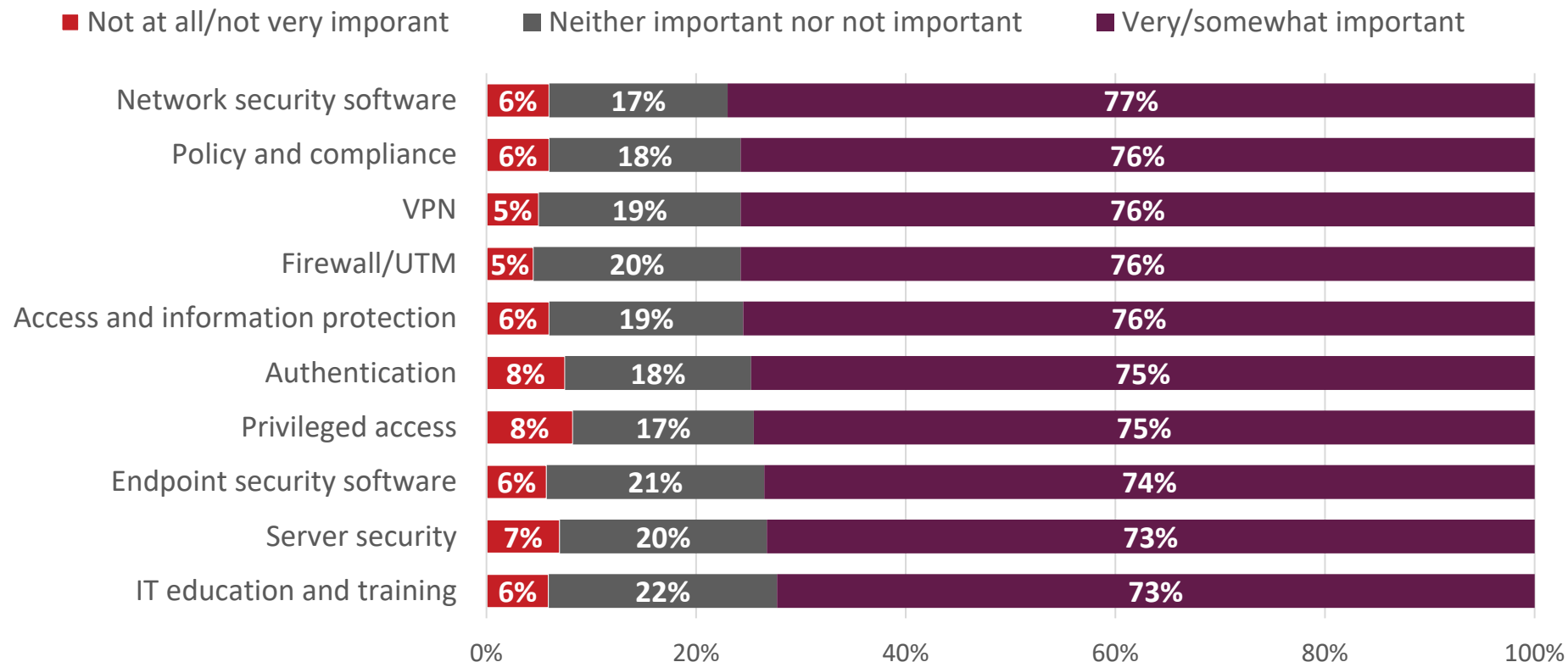
More than half of public sector organizations rate their security posture for fully remote and hybrid employees as improved.



Compared to 2020, how would you rate your organization's overall security posture regarding the following stakeholders?

# Importance of IT Solutions – Top 10 (Slide 1 of 3)

When rating the importance of IT security products, solutions, and services in mitigating risk to the organization, network security software rates highest. Of note, all protocols garnered high importance ratings of 50% and up.



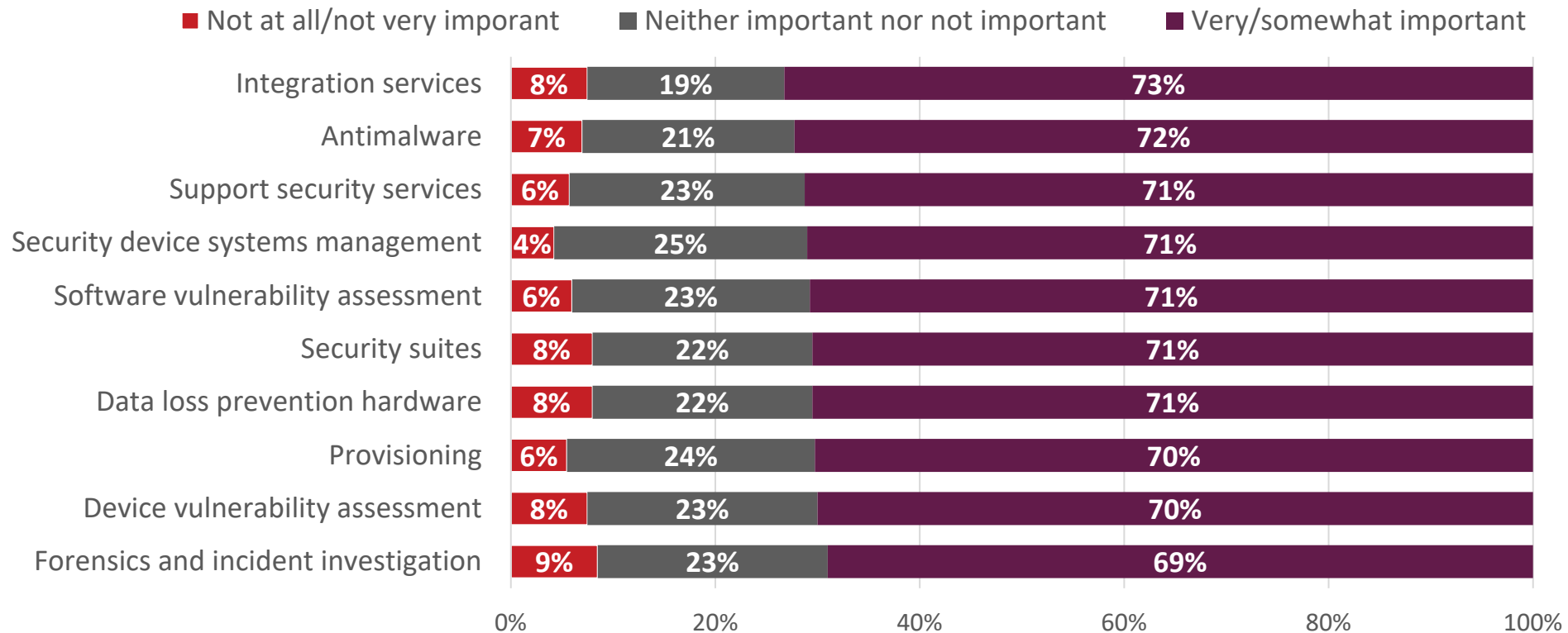
A greater proportion of federal respondents note 19 of the 30 solutions on the survey as important relative to state and local or education respondents.



How important are the following IT security products, solutions, and services in mitigating risk at your organization?

# Importance of IT Solutions (Slide 2 of 3)

When rating the importance of IT security products, solutions, and services, the following 10 protocols were rated in the middle of the IT protocols list.

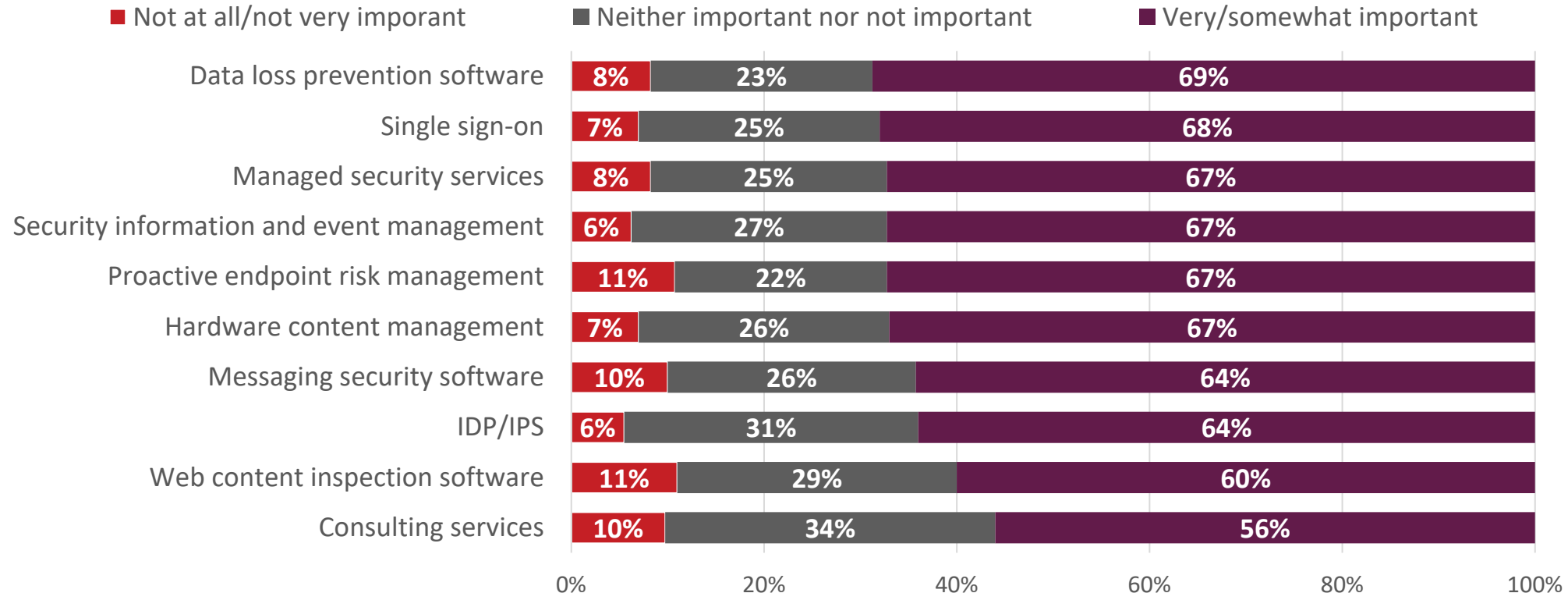


How important are the following IT security products, solutions, and services in mitigating risk at your organization?



# Importance of IT Solutions (Slide 3 of 3)

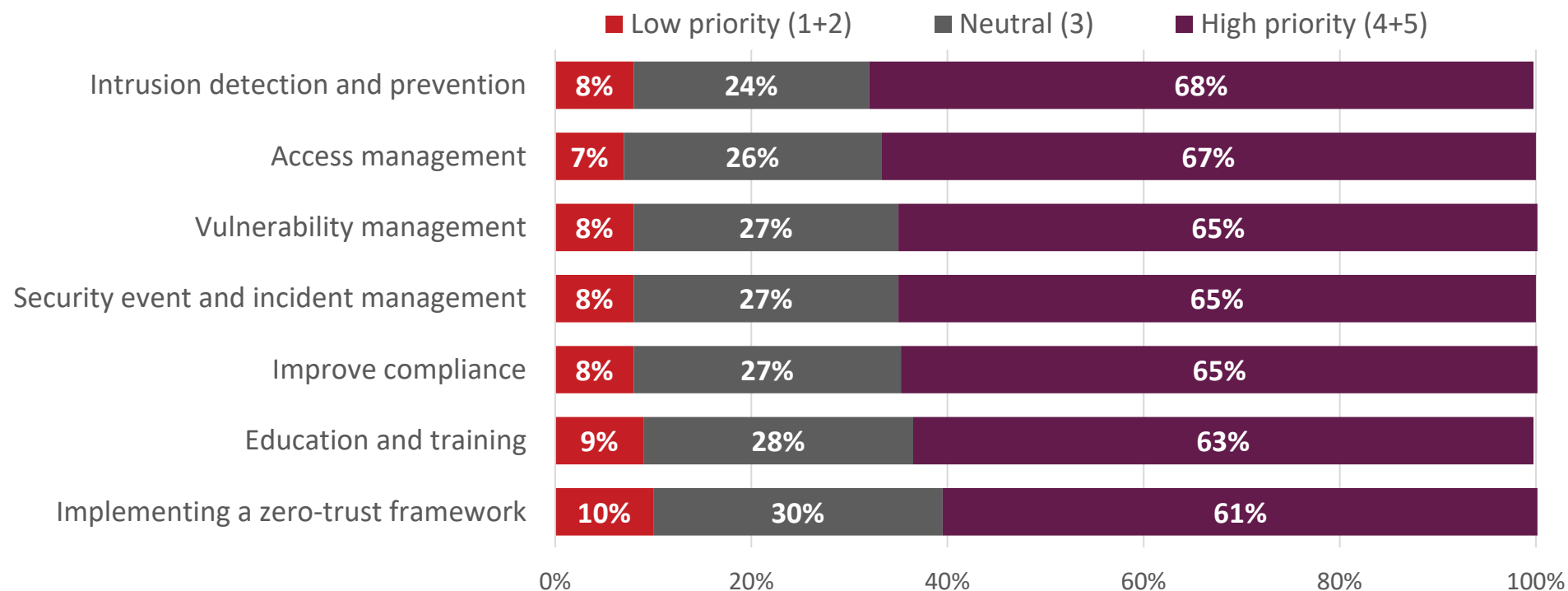
Rating at the bottom of the list of IT protocols is web content inspection software and consulting services.




How important are the following IT security products, solutions, and services in mitigating risk at your organization?

# Investment Priorities: IT Security

Investment priorities for IT security all rate as high priority for public sector organizations, with close to 70% of respondents placing intrusion detection/prevention and access management as their highest priority.



Access management – High Priority 4+5		
Federal	State & Local	Education
64%	63%	76%

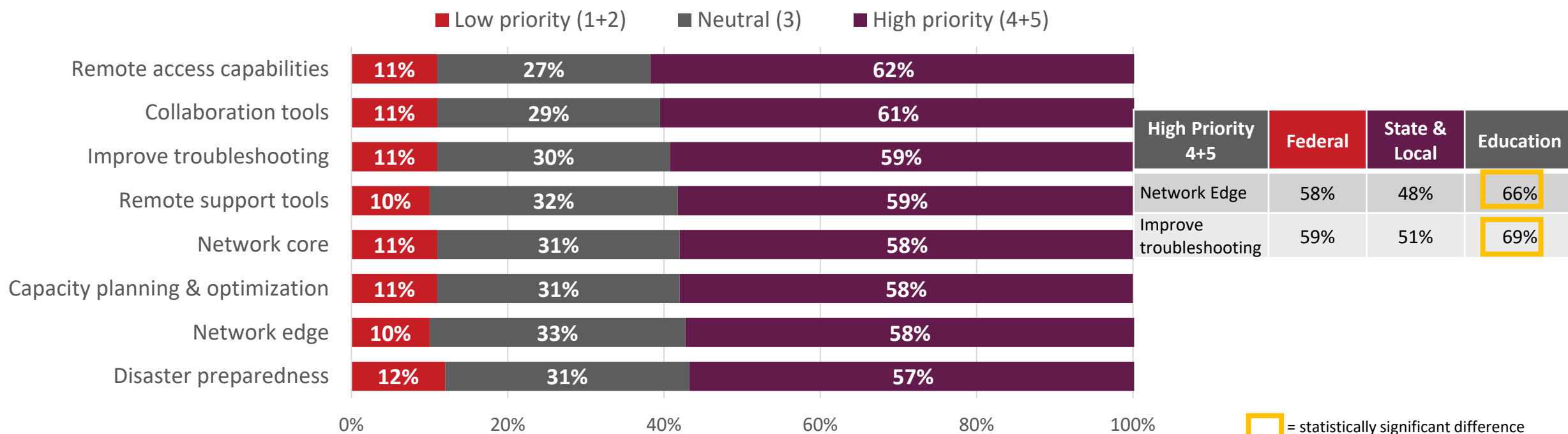
 = statistically significant difference



What are your organization's main investment priorities for the next 12 months (either budget and/or personnel resources)?

# Investment Priorities: Infrastructure

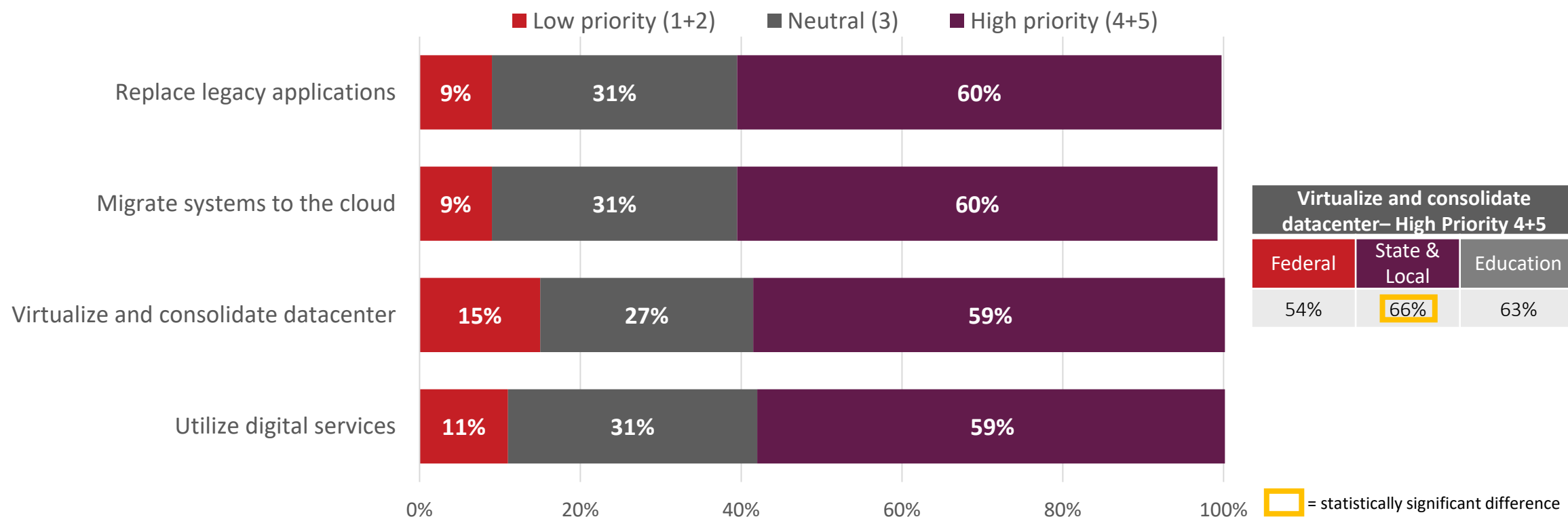
For infrastructure investment, public service organizations place remote access capabilities and collaboration tools as highest priority. All infrastructure investment options hold high priority in general.



What are your organization's main investment priorities for the next 12 months (either budget and/or personnel resources)?

# Investment Priorities: IT Modernization

Like other investment priorities, IT modernization categories rate as high priority. Replacing legacy applications and migrating systems to the cloud hold highest importance.

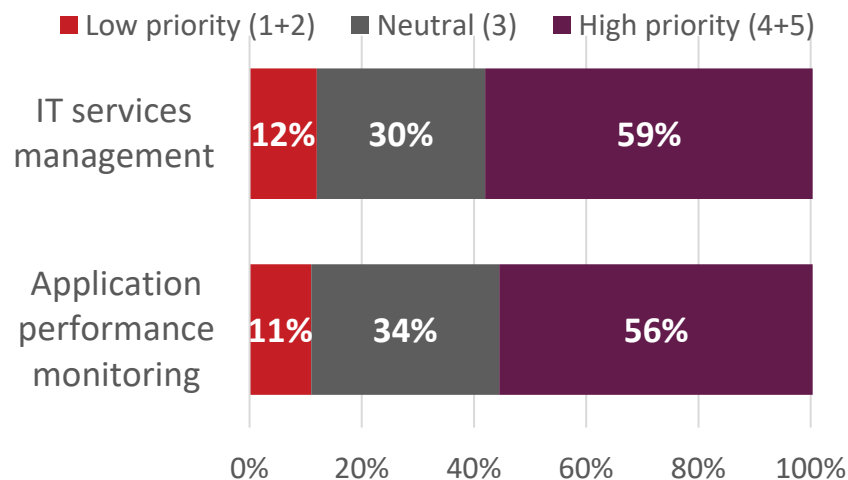


What are your organization's main investment priorities for the next 12 months (either budget and/or personnel resources)?

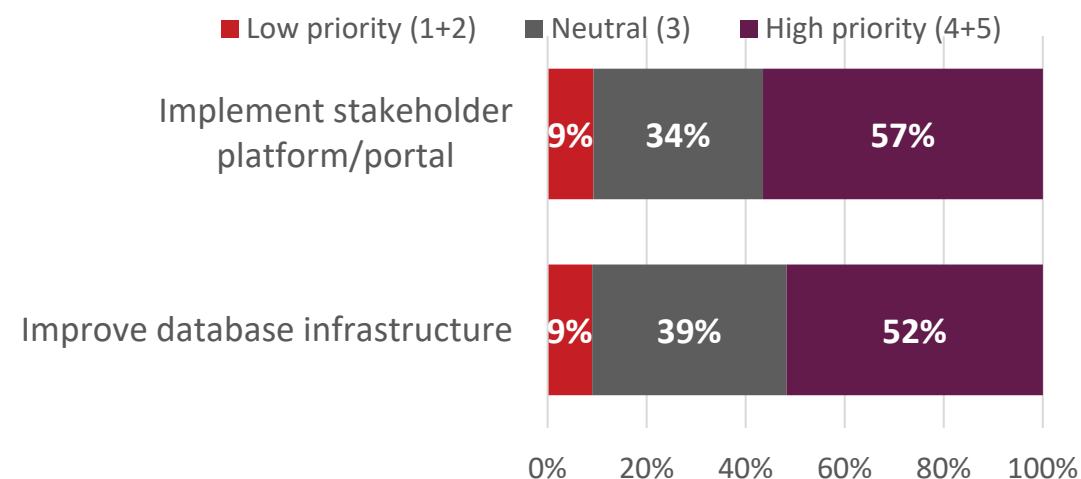
# Investment Priorities: Customer Experience + Digital Transformation

For customer experience investment, IT services management leads. And for digital transformation, implementing stakeholder platforms or portals also rate with priority among public sector organizations.


## Customer Experience



## Digital Transformation



Implement stakeholder platform/portal		
High Priority 4+5		
Federal	State & Local	Education
49%	62%	66%

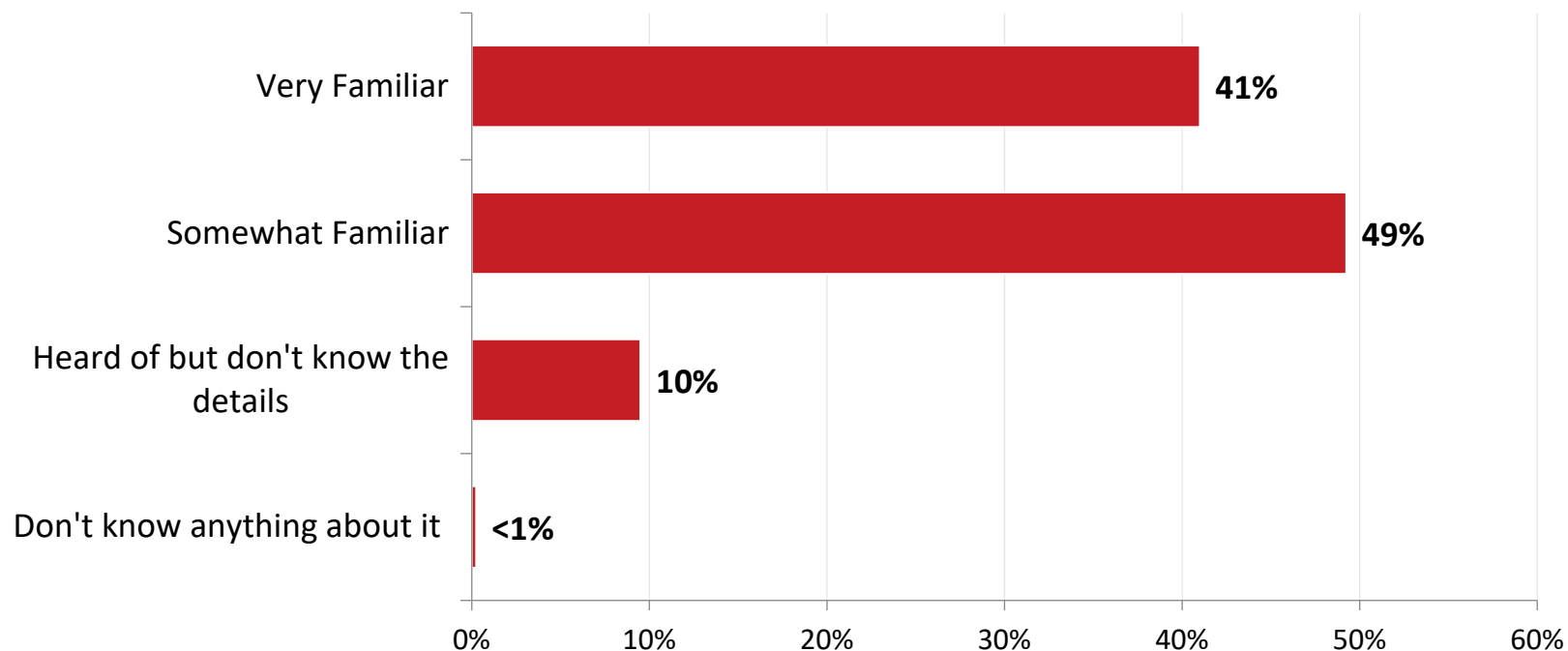
 = statistically significant difference



What are your organization's main investment priorities for the next 12 months (either budget and/or personnel resources)?

# White House Cyber Security Executive Order Familiarity

Most public sector organizations are familiar with the Cyber Security Executive Order. This familiarity is across federal, state and local, and education organizations.

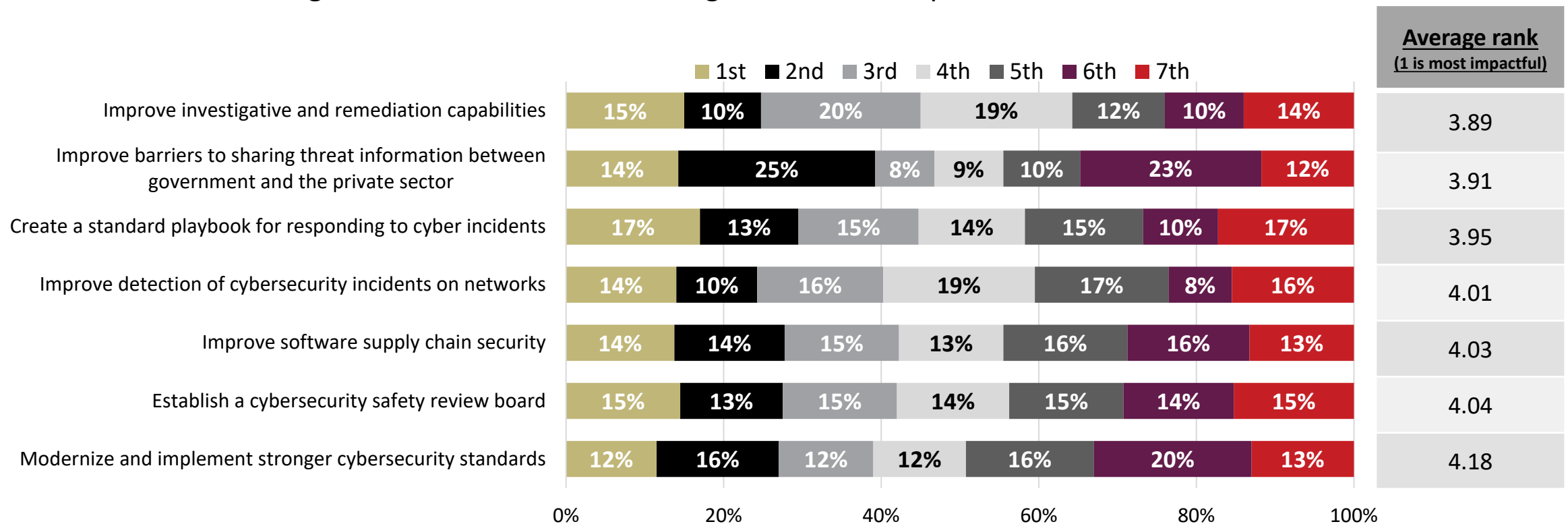



Public and private sector entities increasingly face cyberthreats from a variety of sources. Recent cyber events have resulted in a White House Executive Order to improve the nation's cybersecurity and protect federal government networks. How familiar are you with the Executive Order?



# Executive Order's Impact on Improving Cybersecurity

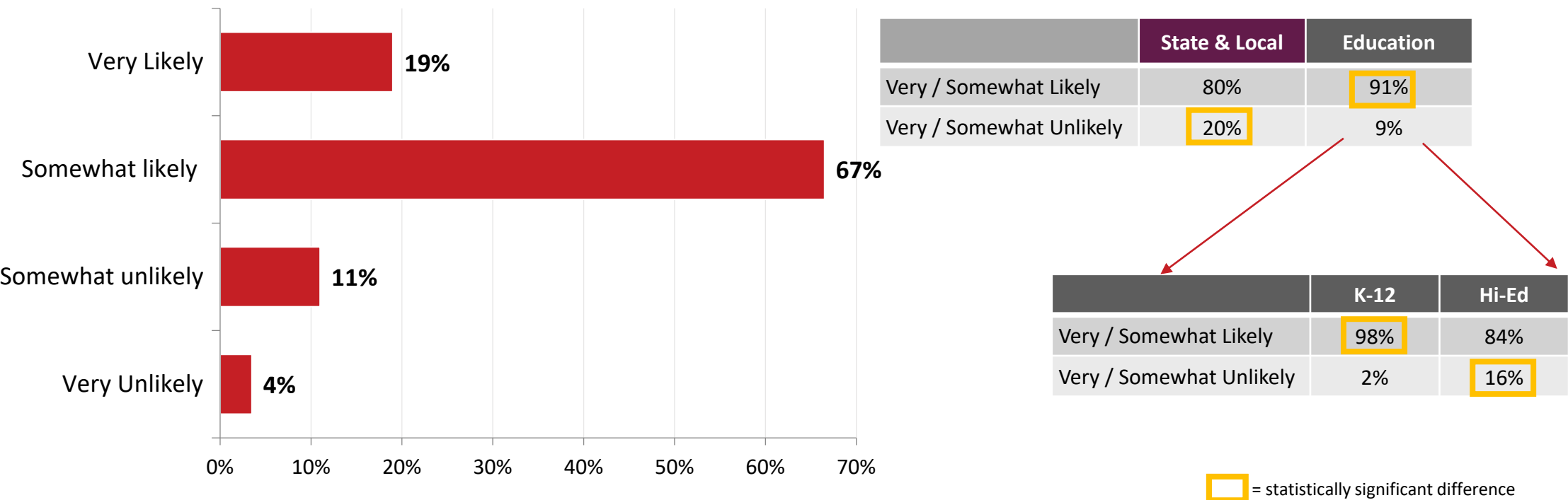
The objectives of the Cyber Security Executive Order that are ranked as most impactful to improving organizations' cybersecurity and network protection are improving investigative and remediation capabilities and improving barriers to sharing threat information between government and private sectors.



 The White House's Cyber Security Executive Order includes multiple objectives. Regardless of your familiarity with the Executive Order, please rank the perceived impact of each objective as it pertains to improving your organization's cybersecurity and network protection. (Rank 1 as the most impactful, 2 is the second most impactful, and so forth.)

# SLED: Likelihood of Incorporating Federal Best Practices

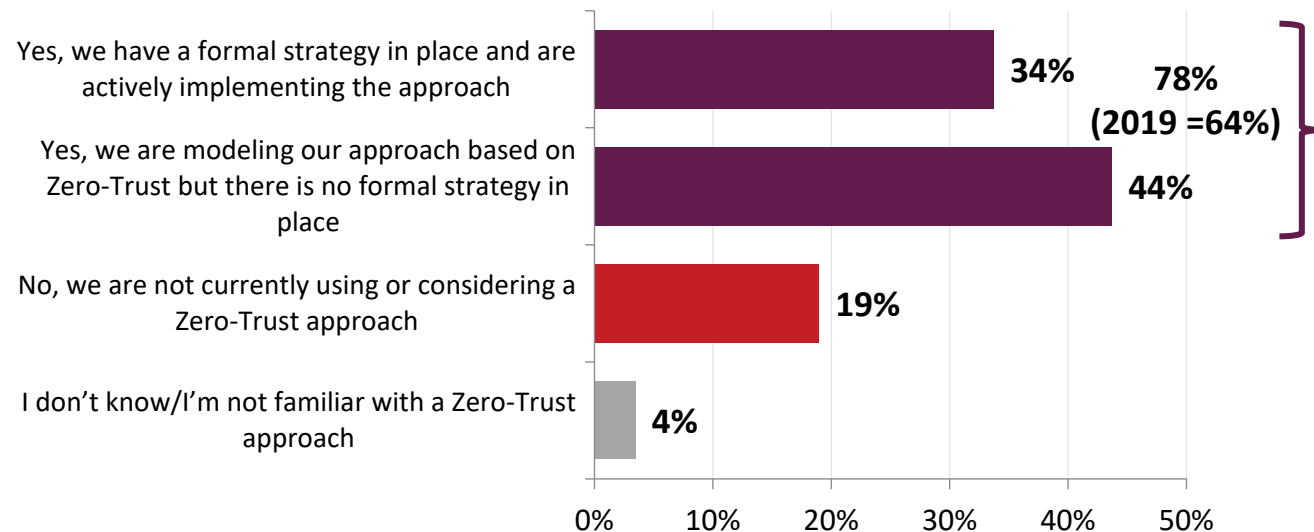
Among state and local governments and education respondents, 86% are likely to refer to or incorporate best practices and activities based on the objectives of the Cyber Security Executive Order. Education organizations, particularly K-12 schools, are significantly more likely to incorporate best practices.



How likely is your organization to refer to or incorporate cybersecurity best practices and activities put forth by the federal government, like those outlined in the Executive Order noted previously?

# Using a Zero-Trust Approach to IT Security – Motivators

More than one-third have a formal strategy in place and are actively implementing the zero-trust approach. Education and defense respondents are more motivated by data protection, local governments by breach protection.



KEY MOTIVATORS	Top 3
Breach protection	70%
Data protection	67%
Reduction of endpoint & IoT security threat	55%
Compliance with the White House Cyber Security Executive Order	36%
Reduce insider threats	35%
Movement to a hybrid cloud environment	29%

	Federal	State & Local	Education	Defense	Civilian	State	Local
Breach protection	71%	73%	67%	70%	71%	61%	82%
Data protection	64%	64%	78%	73%	57%	61%	66%

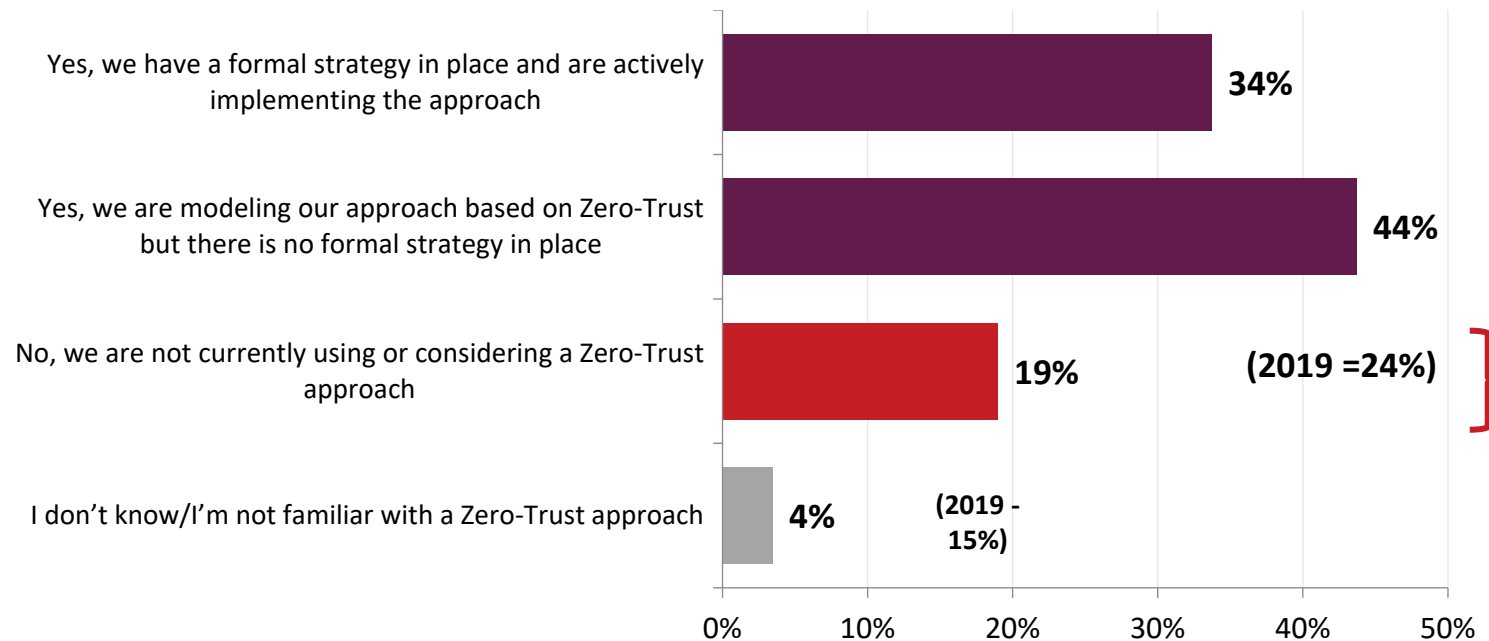


Is your organization currently using or considering a zero-trust approach to IT security? IF YES What are the key motivators for your organization to implement or consider a zero-trust approach?


  = statistically significant difference

# Using a Zero-Trust Approach to IT Security – Deterrents

Nearly one-fifth are not actively using or considering a zero-trust approach. Key deterrents cited are lack of staff expertise, other IT initiatives taking priority, and no formal compliance mandates.



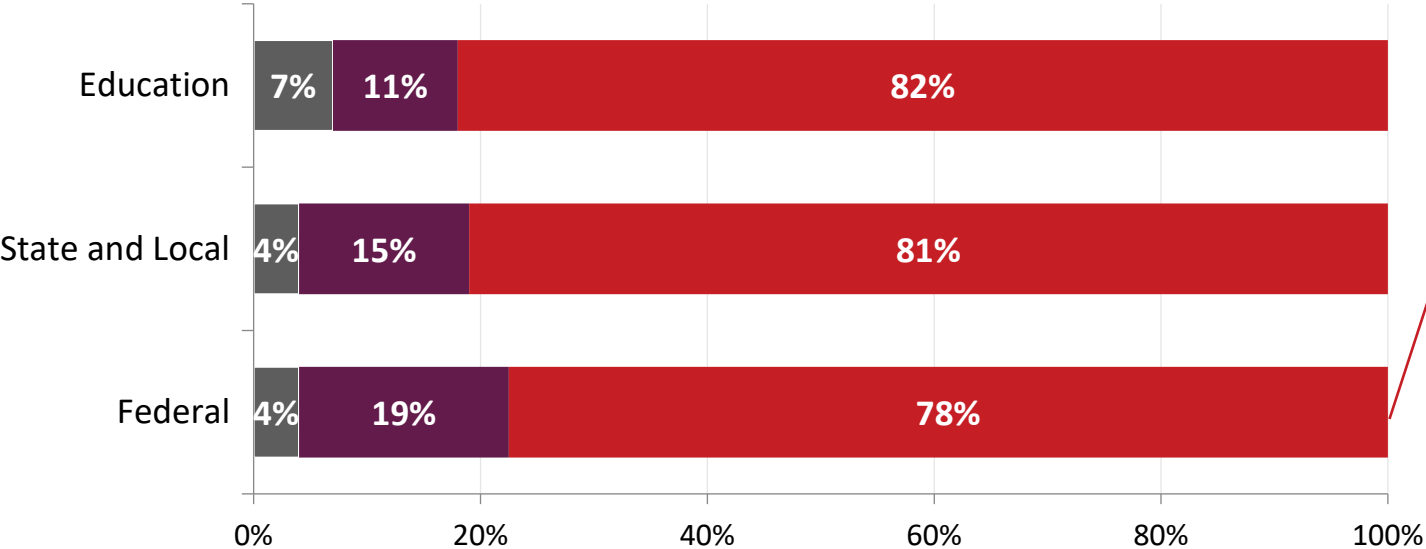
KEY DETERENTS	Top 3
Lack of IT/security staff expertise	57%
Other IT initiatives take priority	55%
No formal compliance mandates	54%
Lack of policies and processes	42%
Solutions are too costly	38%
Leadership/upper management doesn't see the need	30%
Uncertainty over which zero-trust model to follow	24%

 Is your organization currently using or considering a zero-trust approach to IT security? IF NO What are the key deterrents for your organization to implement or consider a zero-trust approach?

# Importance of Zero-Trust Approach

The importance of implementing a zero-trust approach is high among all public sector organizations. Federal civilian respondents are more likely to think zero trust is important to adopt.

■ Not at all/not very important   ■ Neither important nor not important   ■ Very/somewhat important



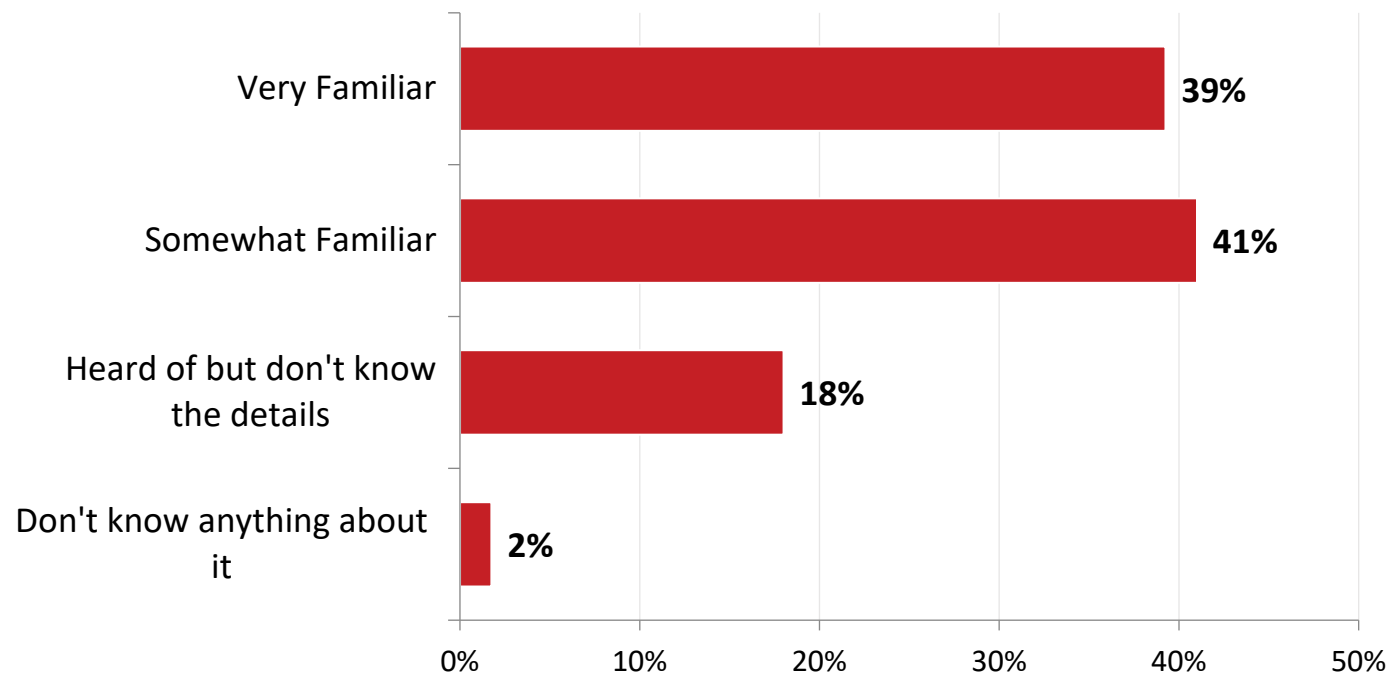
	Defense	Federal Civilian
Very / Somewhat Important	70%	83%
Neither	21%	16%
Very / Somewhat Unlikely	9%	1%

  = statistically significant difference

Regardless of whether you're implementing a zero-trust approach or not, how important is it for [PIPE IN GOVERNMENT AGENICES, EDUCATIONAL INSTITUTIONS, STATE AND LOCAL GOVERNMENTS] to adopt a zero-trust approach?


# Principle of Least Privilege (PoLP) Familiarity


Overall, public sector organizations are familiar with the principle of least privilege, and the education sector is significantly more familiar.



	Federal	State & Local	Education
Familiar	78%	76%	90%
Unfamiliar	23%	24%	10%

	K-12	Hi-Ed
Familiar	84%	96%
Unfamiliar	16%	4%

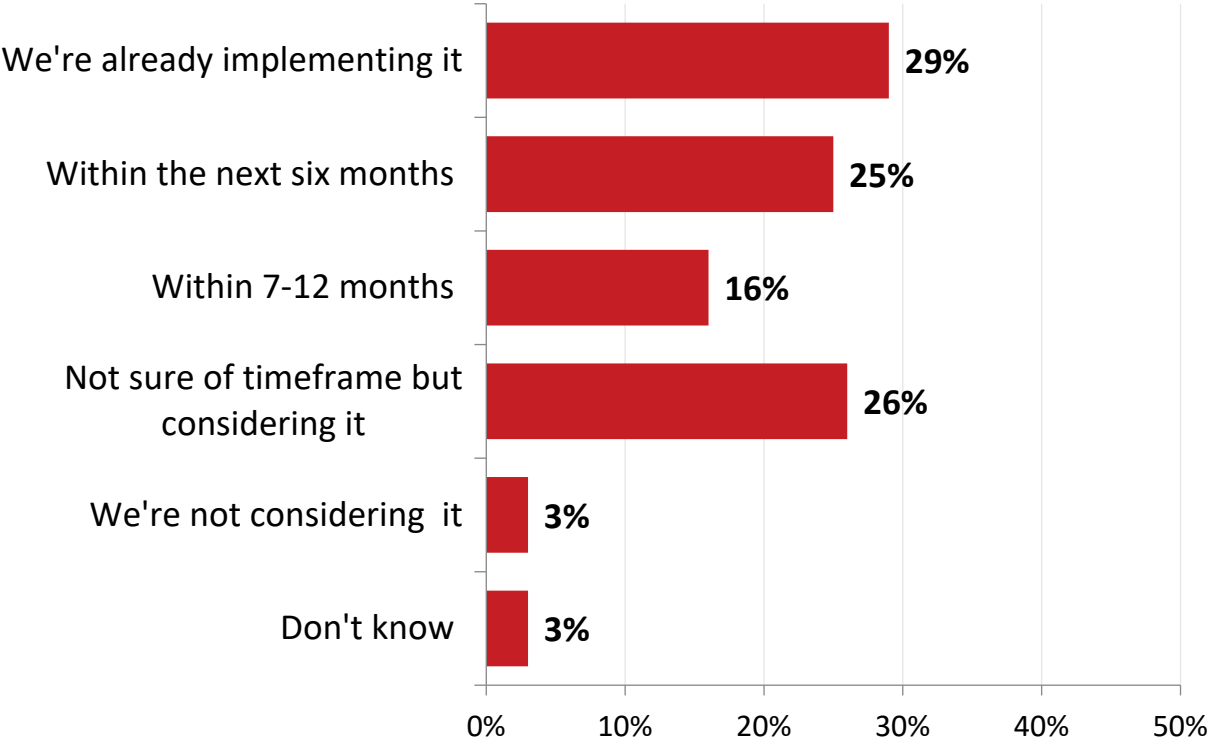
 = statistically significant difference

 A key component of zero trust is the Principle of Least Privilege (PoLP). How familiar are you with the PoLP?



# Timeframe for Implementing PoLP

Nearly one third are actively implementing the principle of least privilege. Reducing the overall attack surface and stopping the spread of malware are the seen as the greatest benefits.



BENEFITS	
Reduces of the overall cyberattack surface	75%
Stops the spread of Malware	72%
Reduces costs by saving time and money in managing users securely	63%
Helps demonstrate compliance with a full audit of privileged activities	50%
Improves end-user productivity	40%

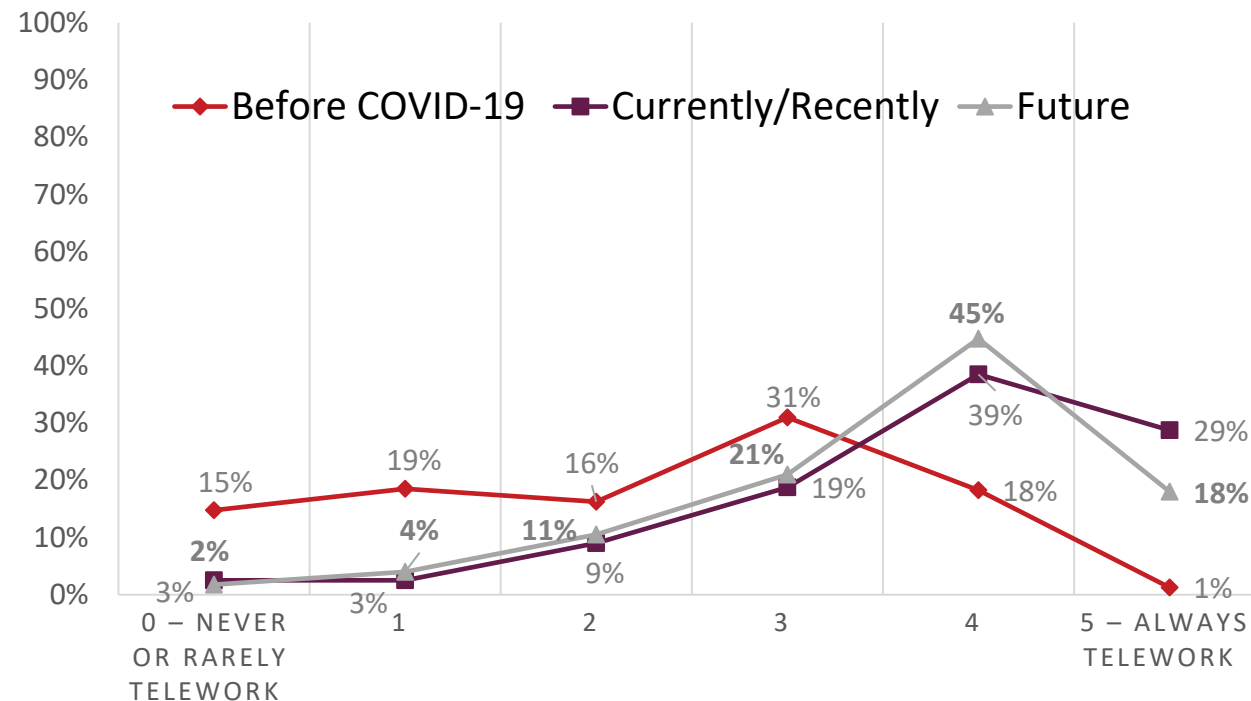
	Federal	State & Local	Education	State	Local
Demonstrates compliance	55%	37%	51%	53%	27%
Stops Malware	69%	78%	73%	63%	88%

= statistically significant difference

What's your estimated timeframe to implement PoLP in your organizations?  
Regardless of whether your organization adheres to the Principle of Least Privilege (PoLP), what do you perceive the top three benefits to be?

# Teleworking - Before COVID-19, Now, and in the Future

Before COVID-19, about half of employees worked remotely sometimes, with close to 20% often/always doing so. Currently, about two-thirds often/always work remotely, and is expected to stay at that level in the future.



MEANS	Before COVID	Currently	Future
<b>Federal</b>	<b>3.12</b>	<b>4.73</b>	<b>4.58</b>
- Defense	2.79	4.39	4.29
- Civilian	3.33	4.96	4.77
<b>State &amp; Local</b>	<b>3.25</b>	<b>4.69</b>	<b>4.51</b>
<b>Education</b>	<b>3.45</b>	<b>4.83</b>	<b>4.62</b>
<b>TOTAL</b>	<b>3.23</b>	<b>4.74</b>	<b>4.57</b>

= statistically significant difference



Please indicate your organization's general level of employee teleworking/working remotely before the COVID-19 pandemic, currently, and how you envision teleworking in the future.

# Representative Comments

“ The main difficulty is in finding and hiring qualified IT employees and then retaining them.

FEDERAL CIVILIAN

“ We are a small agency, so remote work was easier than expected.

FEDERAL CIVILIAN

“ The vast majority of our work is done on classified information systems. As much as we would like to embrace telework or remote operations, it is not physically possible.

DEFENSE / MILITARY

“ A security challenge will be putting trust in hardware that is procured from overseas. The US government’s push for the reshoring of electronics manufacture that began some years ago and has since gained momentum. If you and your customers are based in the United States, reshoring can help alleviate some of the supply chain unknowns. The looming question is how many supply chain unknowns will remain unknown?

DEFENSE / MILITARY

“ We are very concerned about our cybersecurity.

K-12 EDUCATION

“ I think for an organization that has to balance the need to access data remotely due to Covid, plus balance against the need to access a physical office to access certain systems, and the demand from senior leadership to make these systems which should never be remote, remote... rough water are ahead.

FEDERAL CIVILIAN

“ Remote access is improving and will continue to be a priority.

DEFENSE / MILITARY

“ Manpower shortages.

HIGHER EDUCATION



Please feel free to share any other comments or concerns regarding your organization’s unique security challenges or success stories.



# Key Takeaways

The top three sources of security threats remain the same as in previous years.

The greatest increase in concern is from threats from foreign governments.

- Overall, the general hacking community is the largest source of security threat in the public sector. Careless or untrained insiders is still a top three source but has remained stable year over year. Foreign governments is also among the top three sources with more federal government respondents noting it.
- Federal government and SLED respondents' indications of the general hacking community as a threat source has significantly increased.
- Concern about ransomware, malware and phishing has increased for most public sector respondents.



# Key Takeaways

Most public sector respondents realize the importance of IT security solutions and prioritize their investments highly in the next 12 months.

- All IT security solutions received importance ratings of 50% and more. At the very top of the list is network security software. Policy and compliance, VPN, firewall/UTM, and access and information protection all tied for second most important.
- All investment priorities received high priority ratings for public sector organizations. For IT security, almost 70% of respondents placed intrusion detection and prevention and access management top of the list.
- For infrastructure investments, remote access capabilities and collaboration tools were rated as highest priority.
- IT modernization investment priority leans toward replacing legacy applications and migrating systems to the cloud.
- When it comes to customer experience, IT services management holds investment priority. And for digital transformation, implementing stakeholder platforms and portals is key.



# Key Takeaways

Public sector organizations in all segments are aware of the White House Cyber Security Executive Order.

- Ninety percent of respondents are familiar with the White House Cyber Security Executive Order.
- The objectives of the Cyber Security Executive Order that are ranked as most impactful to improving organizations' cybersecurity and network protection are improving investigative and remediation capabilities and improving barriers to sharing threat information between government and private sectors.
- Among SLED organizations, about 20% are very likely and 66% somewhat likely to adopt cybersecurity best practices and activities from the Cyber Security Executive Order. Education organizations are significantly more likely to implement.



# Key Takeaways

The awareness and adoption of zero trust has increased since 2019.

A zero-trust approach is already formally in place or modeled for most organizations because of its key motivators and perceived importance.

- More than three-fourths of public sector organizations use a formal or informal zero-trust approach.
- Motivators for using zero trust include breach protection and data protection, while lack of IT/security staff expertise is the key deterrent.
- All types of public sector organizations give zero trust importance, with federal civilian respondents citing significantly higher importance to the approach.
- Public sector organizations are familiar with the principle of least privilege (PoLP), especially those in education.
- The timeframe of having PoLP in place is already implemented or within the next 12 months for 70% of respondents.



# Key Takeaways

The COVID-19 pandemic drastically changed the work environment for many public sector employees. While some employees have returned to the physical office, respondents expect large numbers teleworking in the future.



- Before COVID-19, about half of employees worked remotely sometimes, with close to 20% often/always doing so.
- Currently, about two-thirds often/always work remotely, and is expected to stay at that level in the future.
- Current and future teleworking is significantly higher for federal civilian organizations.
- More than half of respondents rate their security posture for fully remote and hybrid employees as significantly or somewhat better.



# Contact Information

## **Laurie Morrow, VP, Research Strategy, Market Connections, Inc.**

LaurieM@marketconnectionsinc.com  
571-257-3845

## **Lisa M. Sherwin Wulf, Vice President of Americas Marketing, SolarWinds**

Lisa.SherwinWulf@solarwinds.com  
703-386-2628

## **Jessica Primanzon, Director of Marketing, SolarWinds**

jessica.primanzon@solarwinds.com  
301-672-5351

[www.solarwinds.com/government](http://www.solarwinds.com/government)

LinkedIn: [SolarWinds Government](#)

