SolarWinds Public Sector Cybersecurity Survey Report

February 2020

solarwinds government

Market Connections®
Research you can act on.

Methodology

SolarWinds contracted Market Connections to design and conduct an online survey among 400 public sector IT decision makers and influencers in December 2019 through January 2020. SolarWinds was not revealed as the sponsor of the survey.

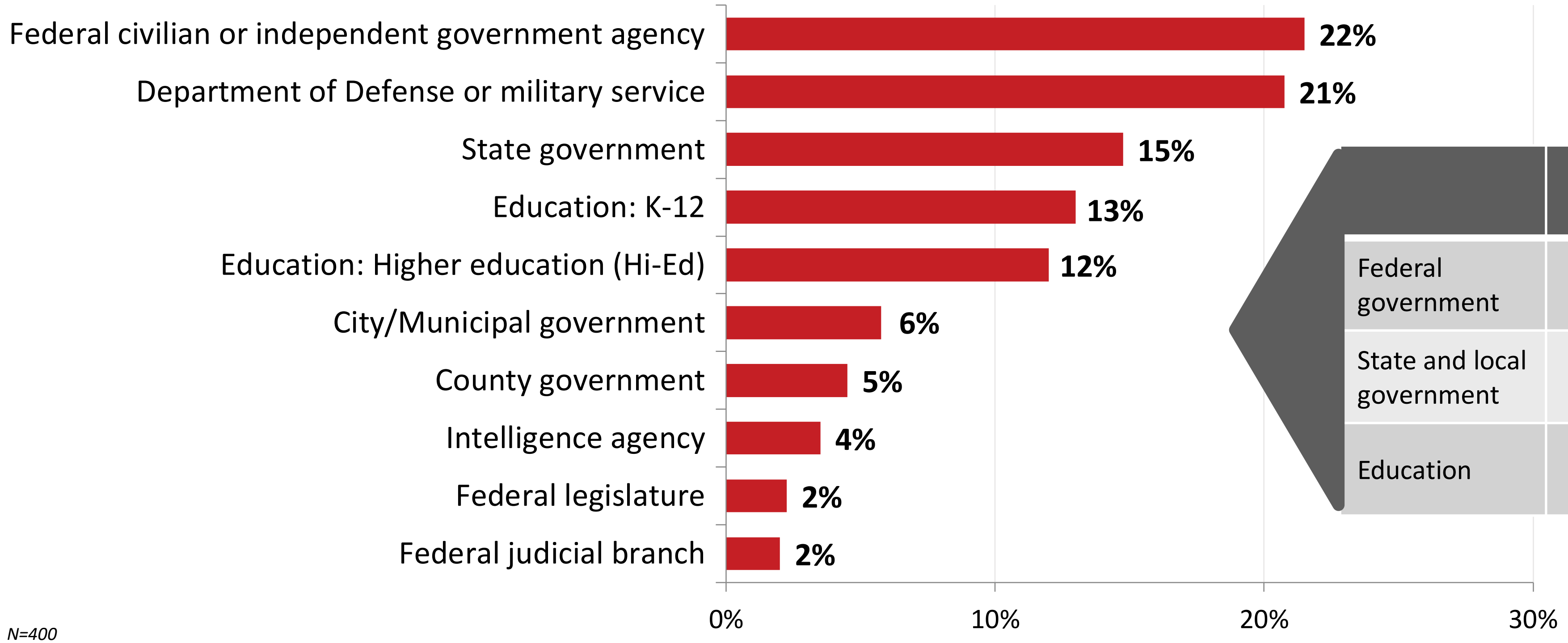
PRIMARY OBJECTIVES:

- Determine challenges faced by public sector IT professionals and sources of IT security threats
- Evaluate cybersecurity capabilities and factors that have impacted IT security and policies
- Identify IT team structures, how IT security operations are sourced, and their level of success
- Determine if organizations segment users by risk level, the challenges associated with segmentation, and the perceived risk associated with different user types
- Identify privileged users and if organizations are using a Zero-Trust approach to IT security

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.

Organization Type



	Count	Percent
Federal government	200	50%
State and local government	100	25%
Education	100	25%

N=400

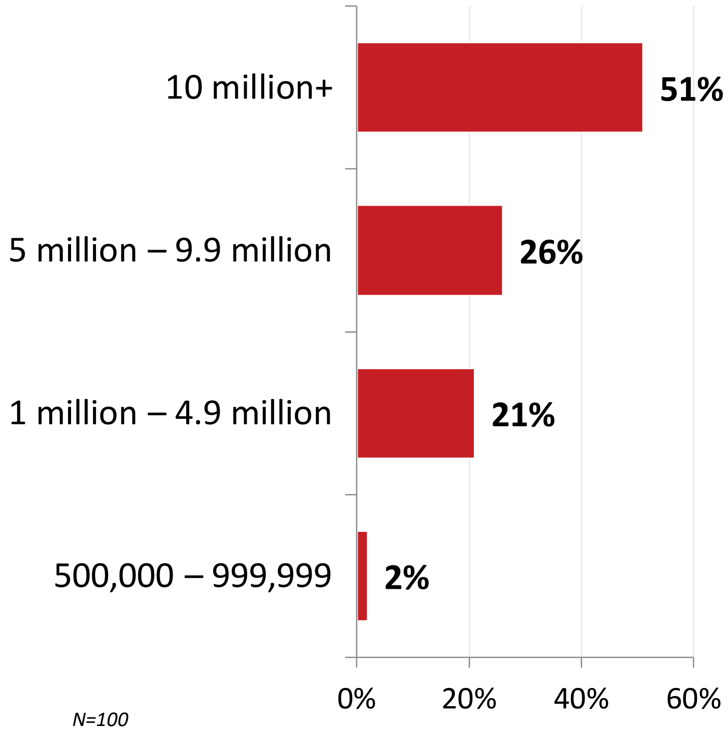
Q *Which of the following best describes your current employer?*

RESPONDENT CLASSIFICATIONS

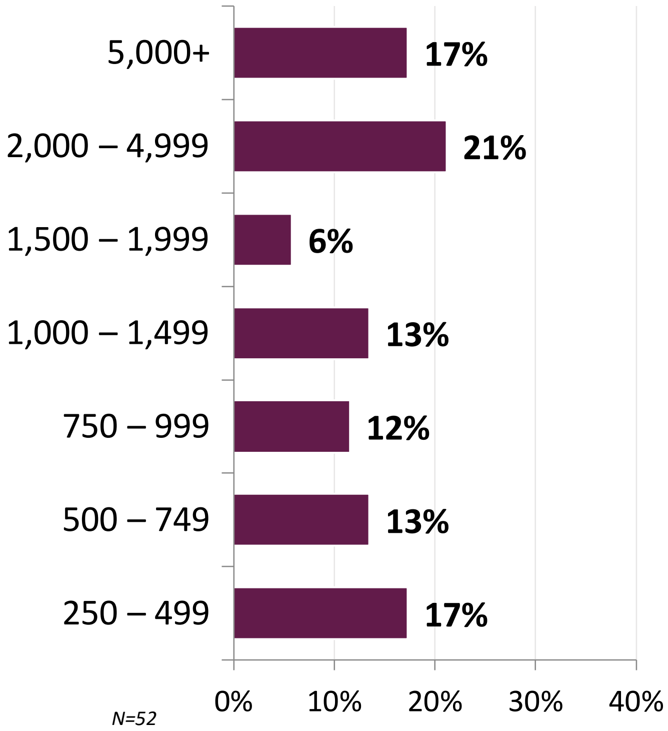
SLED Population and Enrollment

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.

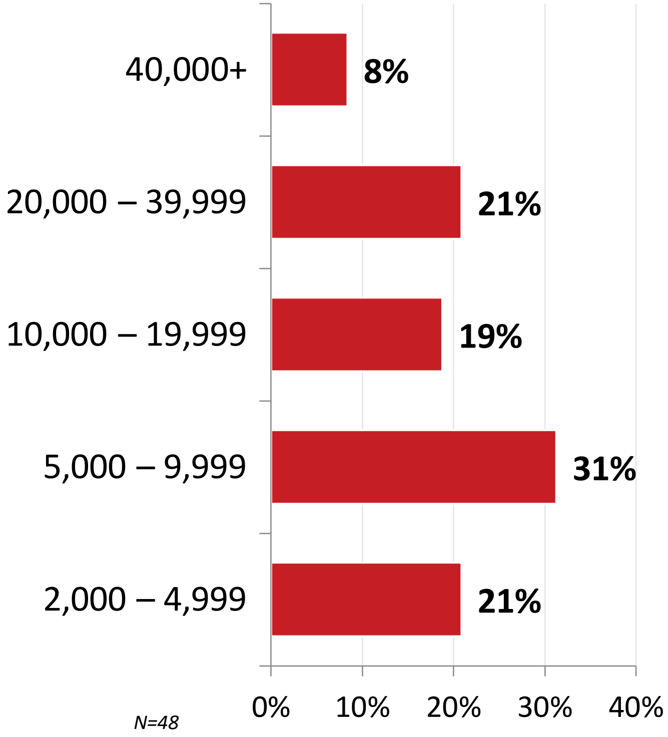
State and Local Population



K-12 Enrollment



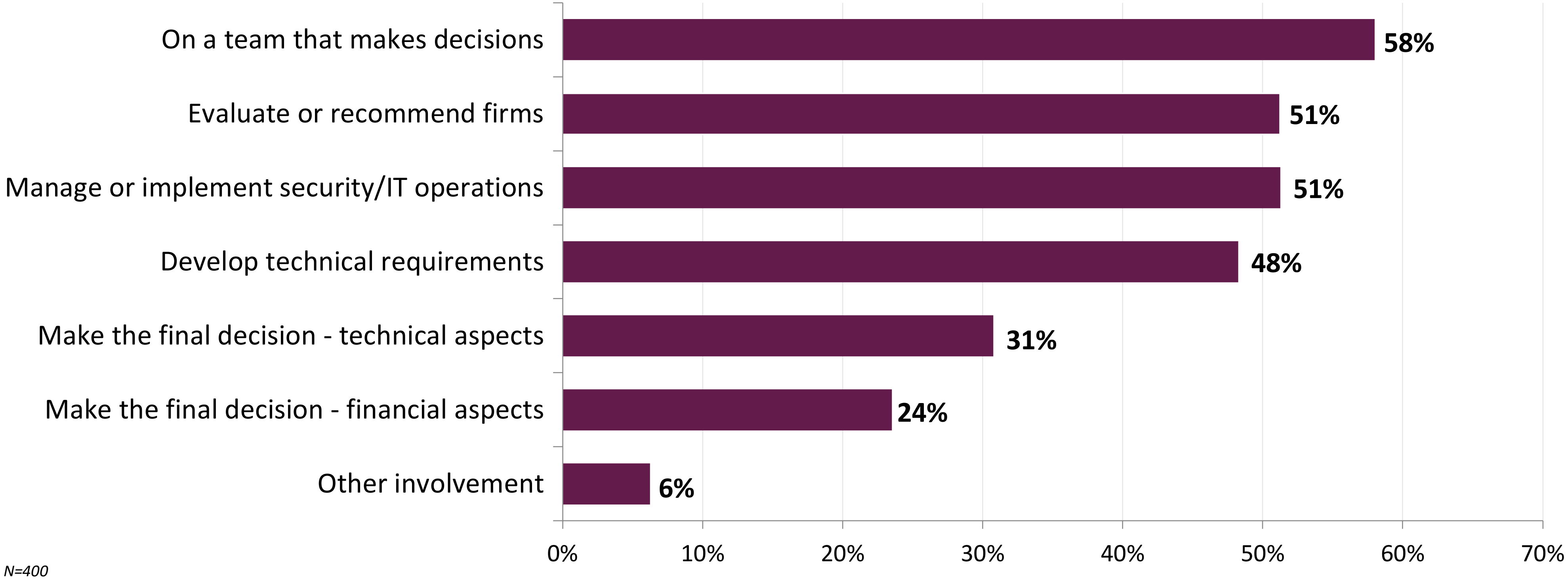
Higher Education Enrollment



Q *[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.

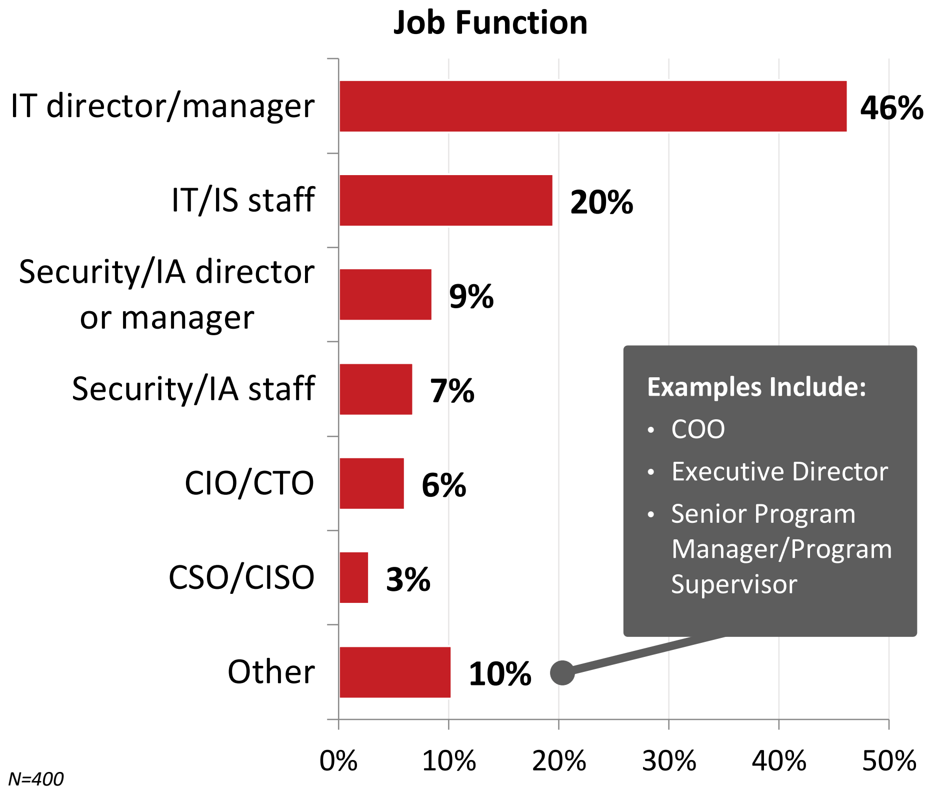


N=400
Note: Multiple responses allowed

Q *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)*

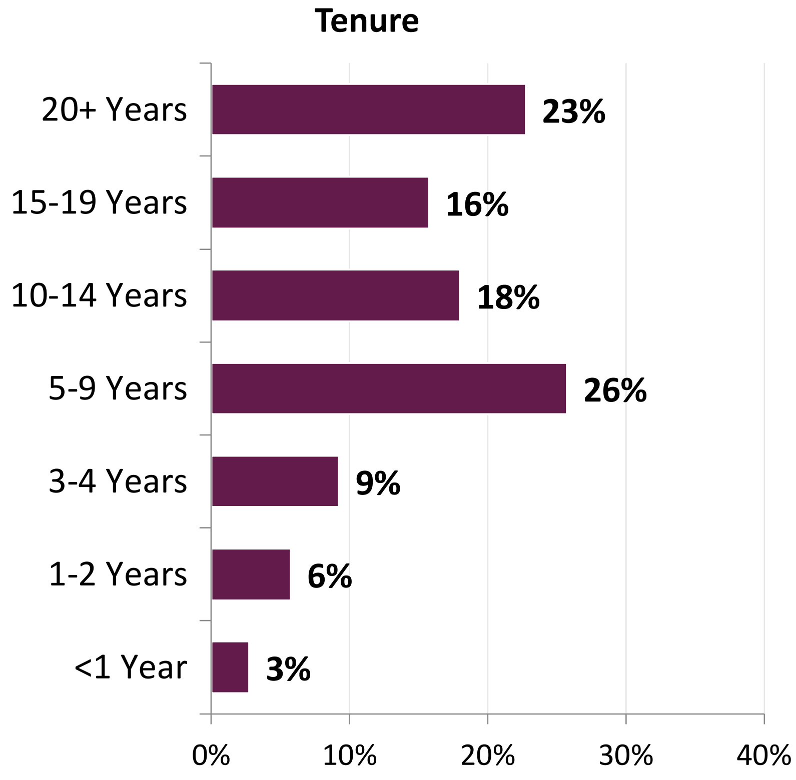
Job Function and Tenure

A variety of job functions and tenures are represented in the sample, with most being IT management and working at their current organization for 5-9 years, followed by a large proportion working 20+ years.



Examples Include:

- COO
- Executive Director
- Senior Program Manager/Program Supervisor

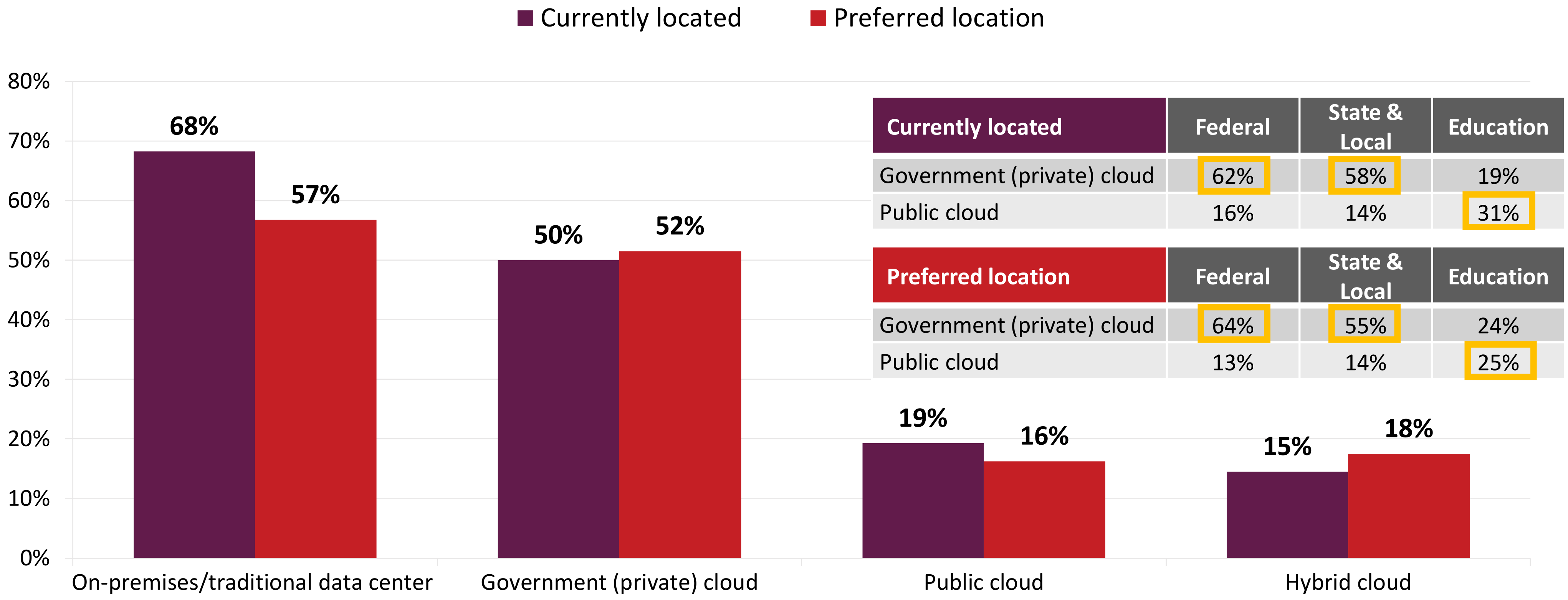


N=400

Q *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 similar to the current location.



Currently located	Federal	State & Local	Education
Government (private) cloud	62%	58%	19%
Public cloud	16%	14%	31%

Preferred location	Federal	State & Local	Education
Government (private) cloud	64%	55%	24%
Public cloud	13%	14%	25%

N=400
Note: Multiple responses allowed

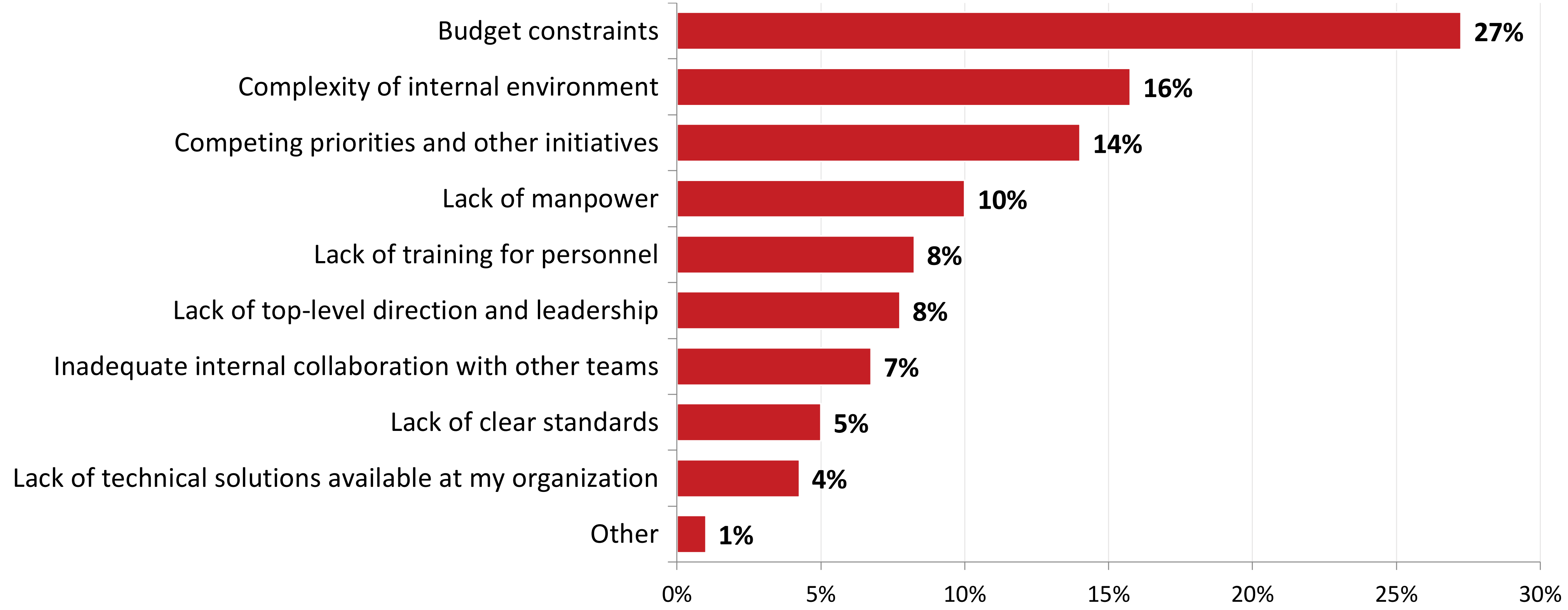
□ = statistically significant difference

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

solarwinds

IT Security Obstacles

Budget constraints top the list of significant obstacles to maintaining or improving organization IT security.



N=400

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

solarwinds

IT Security Obstacles by Organization Type

Education respondents indicate more so than other public sector groups that budget constraints (driven by K-12) and lack of training for personnel are obstacles to maintaining or improving IT security.

Federal respondents indicate the complexity of the internal environment more than other public sector respondents.

While budget constraints have declined since 2014 for the federal audience, the complexity of the internal environment as an obstacle has increased.

	K-12	Hi-Ed
Budget constraints	□ 44%	25%

	Federal	State & Local	Education
Budget constraints	24%	27%	□ 35%
Complexity of internal environment	□ 21%	13%	8%
Lack of training for personnel	6%	7%	□ 14%

Federal	2014	2019
Budget constraints	40%	24% ↓
Complexity of internal environment	14%	21% ↑

N=400

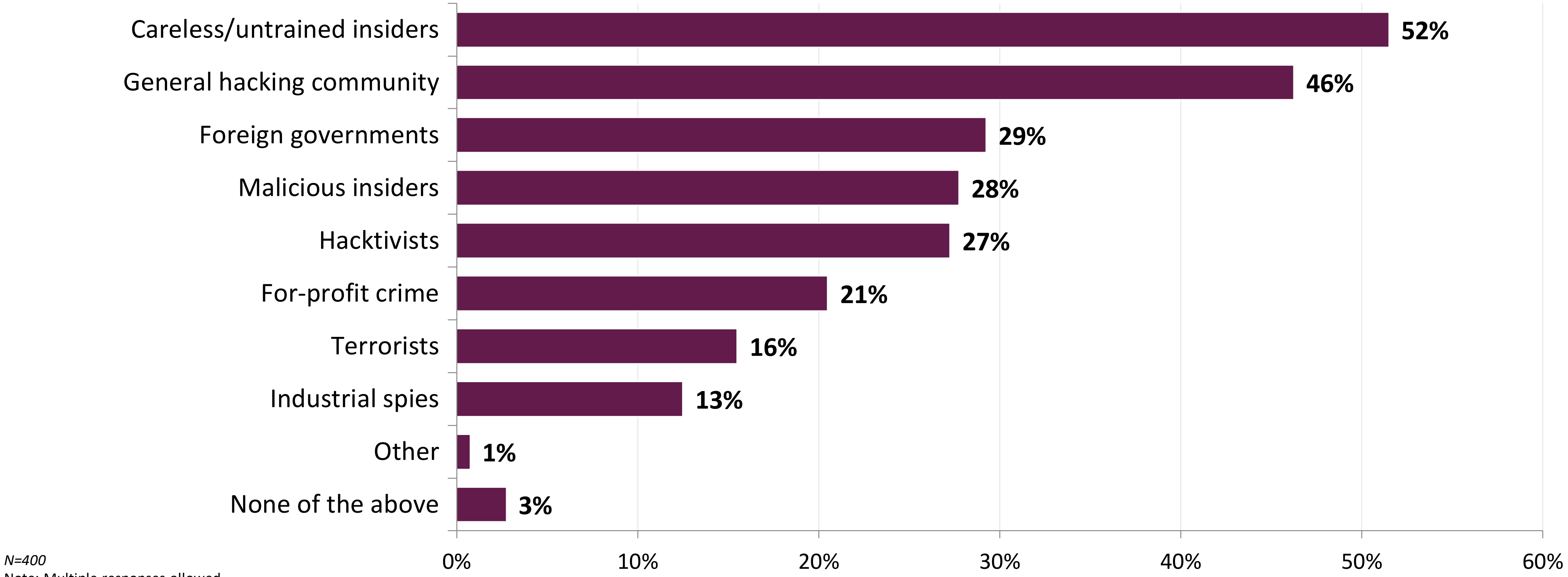
□ = statistically significant difference

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

solarwinds

Sources of Security Threats

Careless/untrained insiders are noted as the largest source of security threats at public sector organizations.



N=400

Note: Multiple responses allowed

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

Sources of Security Threats by Organization Type

Education respondents note the general hacking community as a source of security threats significantly more so than other public sector groups. More federal civilians than defense also note the general hacking community.

Federal and state and local respondents (particularly state respondents) indicate foreign governments as a threat more so than education respondents indicate.

Significantly more federal (particularly defense) and state and local respondents than education indicate terrorists as a threat.

For careless/untrained insiders (the top source of threats overall), there are no significant differences between organization types.

	Federal	State & Local	Education
General hacking community	40%	51%	**54%**
Foreign governments	**48%**	**18%**	4%
Terrorists	**22%**	**15%**	3%

	State	Local
Foreign governments	**25%**	7%

	Defense	Civilian
General hacking community	33%	**47%**
Terrorists	**30%**	15%

N=400
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 no significant changes from 2018 to 2019.

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

N=200
Note: Multiple responses allowed

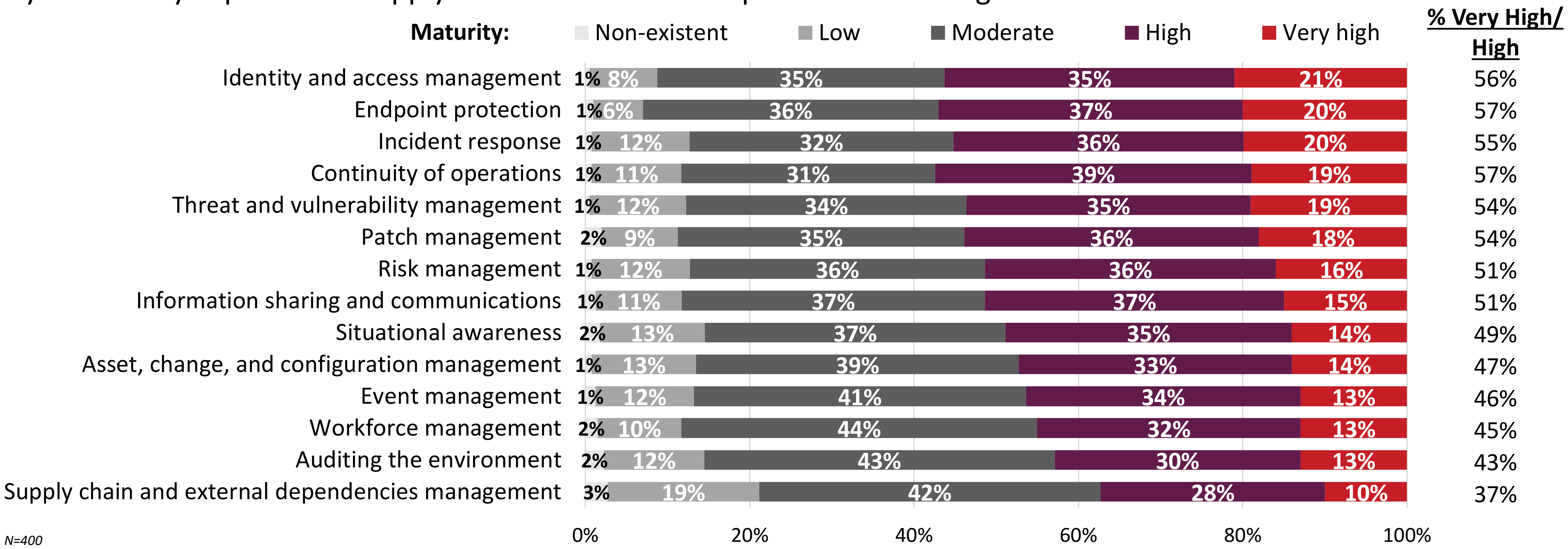
🟪 = top three sources

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

solarwinds

Organization Maturity

Identity and access management and endpoint protection are rated highest in terms of organization maturity of its cybersecurity capabilities. Supply chain and external dependencies management is rated the lowest.



N=400

Q *Thinking about your organization's maturity of its cybersecurity capabilities, how would you rate each of the following?*

Organization Maturity by Organization Type

Federal respondents' ratings are significantly more mature than state and local and education respondents in many cybersecurity capabilities. State respondents also tend to be more mature in their capabilities than local respondents. Hi-Ed respondents are more mature than K-12.

% Very High/High	Federal	State & Local	Education
Identity and access management	65%	53%	42%
Endpoint protection	65%	53%	45%
Incident response	64%	53%	40%
Continuity of operations	64%	48%	53%
Threat and vulnerability management	64%	46%	41%
Patch management	61%	49%	45%
Risk management	59%	46%	41%
Information sharing and communications	57%	48%	44%
Situational awareness	57%	40%	43%
Asset, change, and configuration management	57%	33%	43%
Event management	53%	42%	37%
Workforce management	53%	38%	36%
Auditing the environment	51%	36%	34%

N=400

% Very High/High	State	Local
Identity and access management	63%	39%
Patch management	58%	37%
Supply chain and external dependencies management	42%	17%

% Very High/High	K-12	Hi-Ed
Identity and access management	33%	52%
Incident response	29%	52%
Continuity of operations	40%	67%
Threat and vulnerability management	31%	52%
Patch management	35%	56%
Risk management	31%	52%
Information sharing and communications	31%	58%
Asset, change, and configuration management	33%	54%
Workforce management	27%	46%

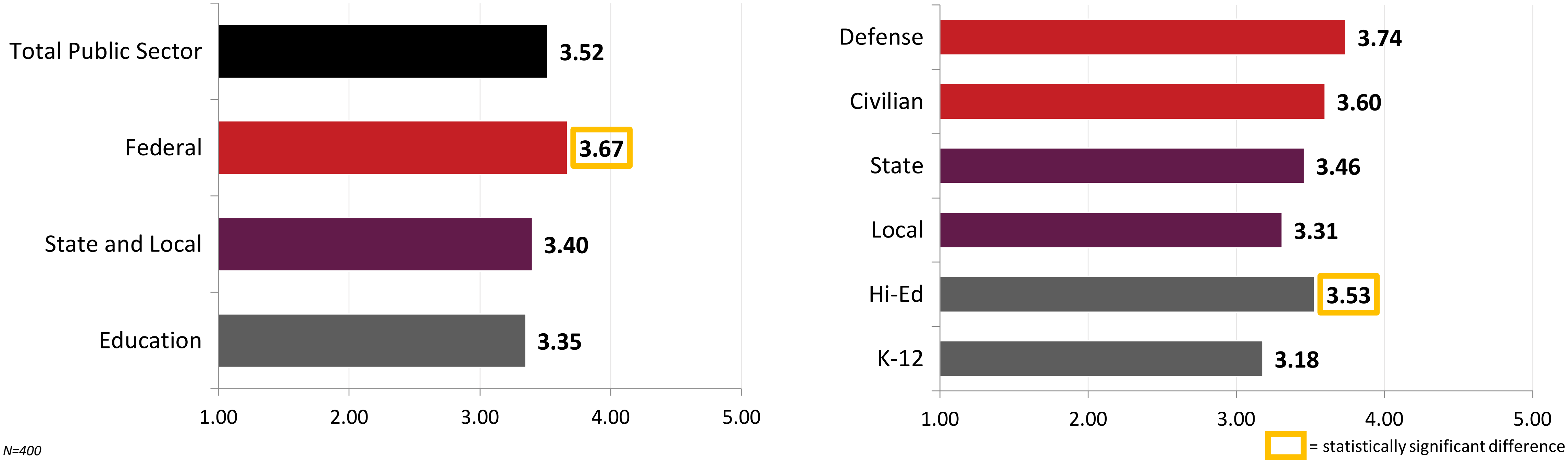
□ = statistically significant difference

Q *Thinking about your organization's maturity of its cybersecurity capabilities, how would you rate each of the following?*

Average Organization Maturity by Organization Type

When averaging all cybersecurity maturity ratings, federal respondents are overall significantly more mature than state and local and education respondents. For education, Hi-Ed is significantly more mature than K-12.

Average Organization Maturity (1=Non-Existent, 5=Very High)

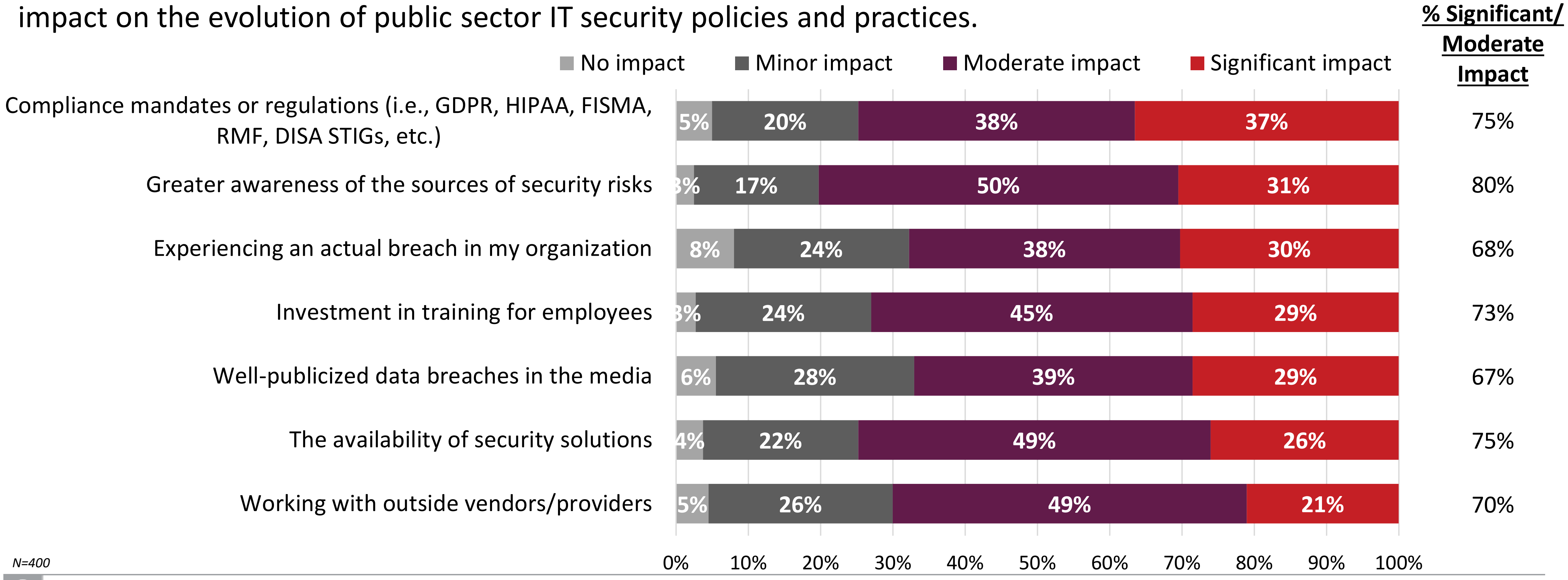


N=400

Thinking about your organization's maturity of its cybersecurity capabilities, how would you rate each of the following?

Impacts on the Evolution of IT Security Policies

Compliance mandates or regulations and a greater awareness of the sources of security risks have had the greatest impact on the evolution of public sector IT security policies and practices.



N=400

Q *What impact do you think the following factors have had on your organization's evolution of its IT security policies and practices?*

Impacts on IT Security Policies by Organization Type

Significantly more federal than other public sector respondents think compliance mandates or regulations and investment in training for employees have impacted their organization's evolution of its IT security policies and practices.

% Significant/Moderate Impact	Federal	State & Local	Education
Compliance mandates or regulations	79%	68%	73%
Investment in training for employees	77%	72%	66%

A larger proportion of defense than civilian respondents think greater awareness of the sources of security risks and investment in training for employees have had an impact.

% Significant/Moderate Impact	Defense	Civilian
Greater awareness of the sources of security risks	88%	76%
Investment in training for employees	84%	71%

More state respondents than local indicate compliance mandates or regulations have had an impact.

% Significant/Moderate Impact	State	Local
Compliance mandates or regulations	80%	51%

A larger proportion of Hi-Ed than K-12 respondents indicate the availability of security solutions.

% Significant/Moderate Impact	K-12	Hi-Ed
The availability of security solutions	65%	83%

N=400

□ = statistically significant difference

What impact do you think the following factors have had on your organization's evolution of its IT security policies and practices?

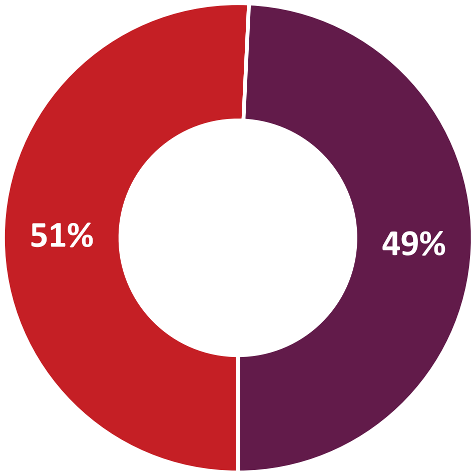
solarwinds

IT Operations and IT Security Structure

When describing their organization’s IT operations/infrastructure team and IT security team, public sector respondents overall are split with about half having separate departments and half being within the same department. Most federal respondents indicate they have separate departments, education indicates the same department, and state and local are split between either having a separate or being within the same department.

🟥 We have separate departments or teams with different staff and purpose.

🟪 Our IT security efforts are absorbed by IT personnel within the same department.



	Federal	State & Local	Education
We have separate departments or teams with different staff and purpose	61%	50%	31%
Our IT security efforts are absorbed by IT personnel within the same department	40%	50%	69%

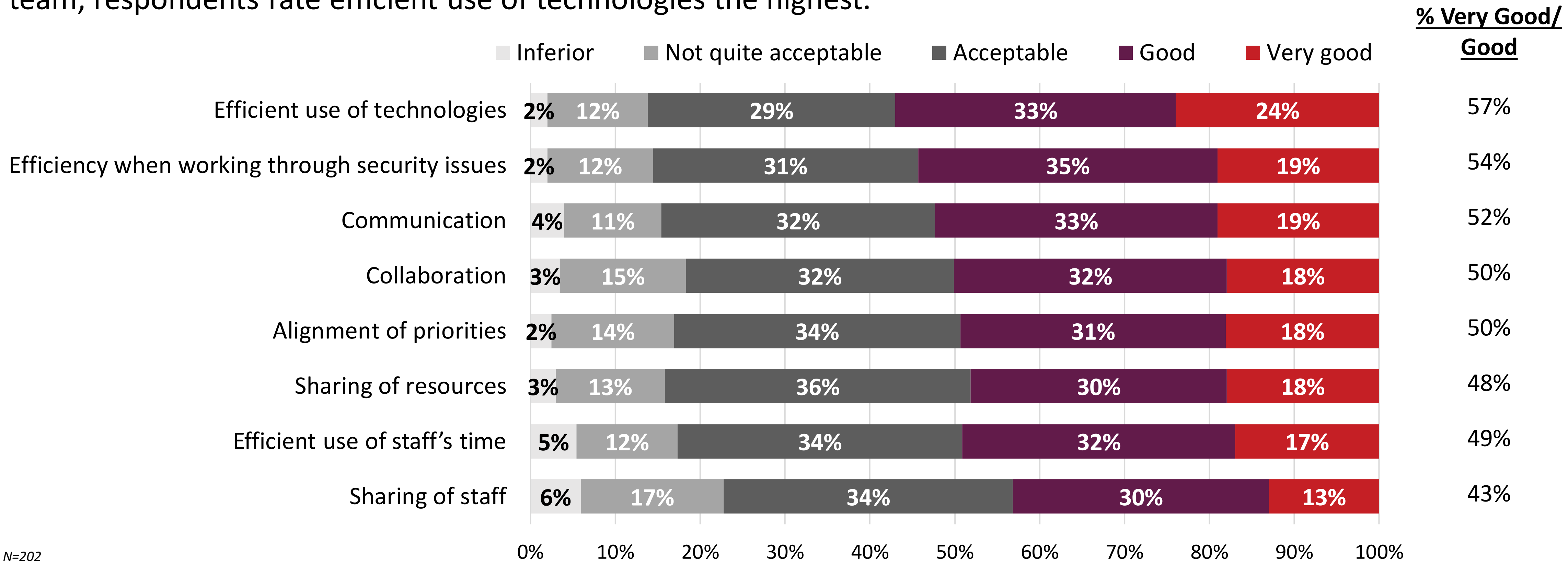
□ = statistically significant difference

N=400

Which statement best describes your organization’s IT operations/infrastructure team and IT security team?

IT Operations and IT Security Teams Relationship

When rating their organization’s IT operations/infrastructure team’s working relationship with their IT security team, respondents rate efficient use of technologies the highest.

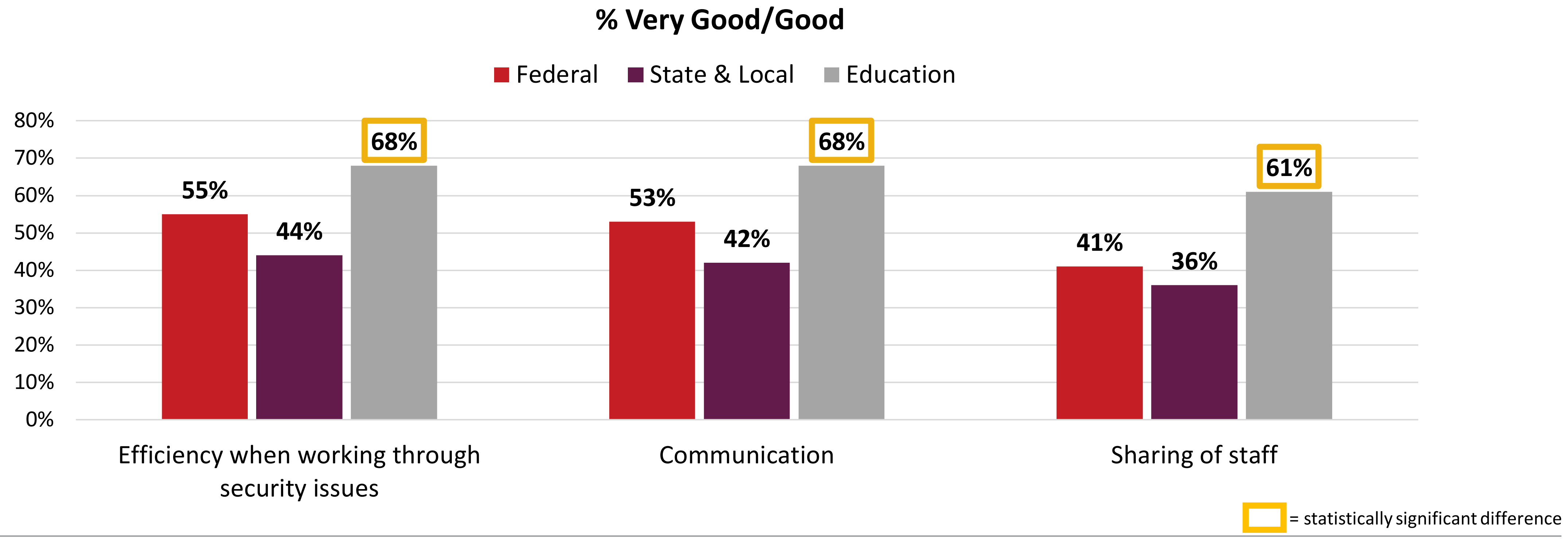


N=202

Overall, how would you rate your organization’s IT operations/infrastructure team’s working relationship with your IT security team on the following factors?

IT Operations and IT Security Relationship by Organization Type

Education respondents rate efficiency when working through security issues, communication, and sharing of staff higher than ratings from federal and state and local respondents.

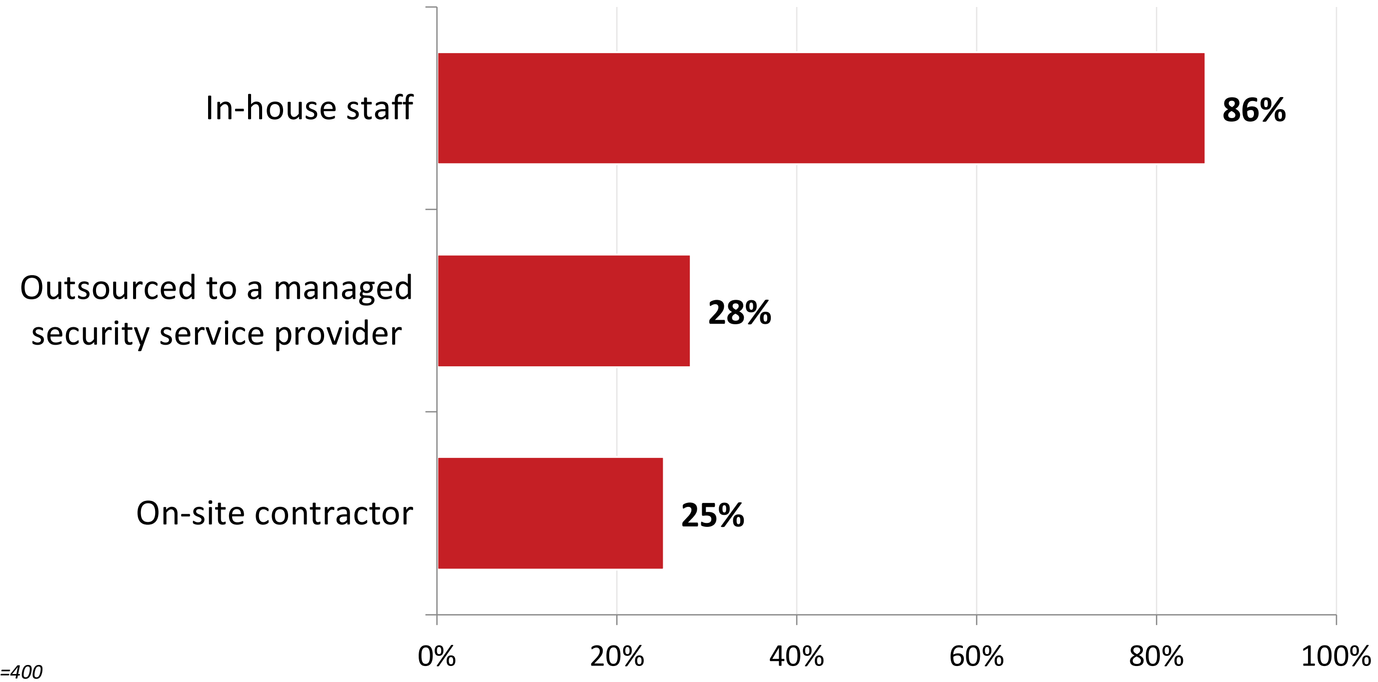


N=202

Overall, how would you rate your organization's IT operations/infrastructure team's working relationship with your IT security team on the following factors?

Organization’s IT Security Operations

The majority, and significantly more so for state and local, indicate their organization's IT security operations are sourced through in-house staff. More federal than other public sector respondents use an on-site contractor. Local respondents are more likely than state to outsource to a managed service provider.



	Federal	State & Local	Education
In-house staff	82%	91%	87%
On-site contractor	41%	9%	10%

	State	Local
Outsourced to a managed security service provider	15%	39%

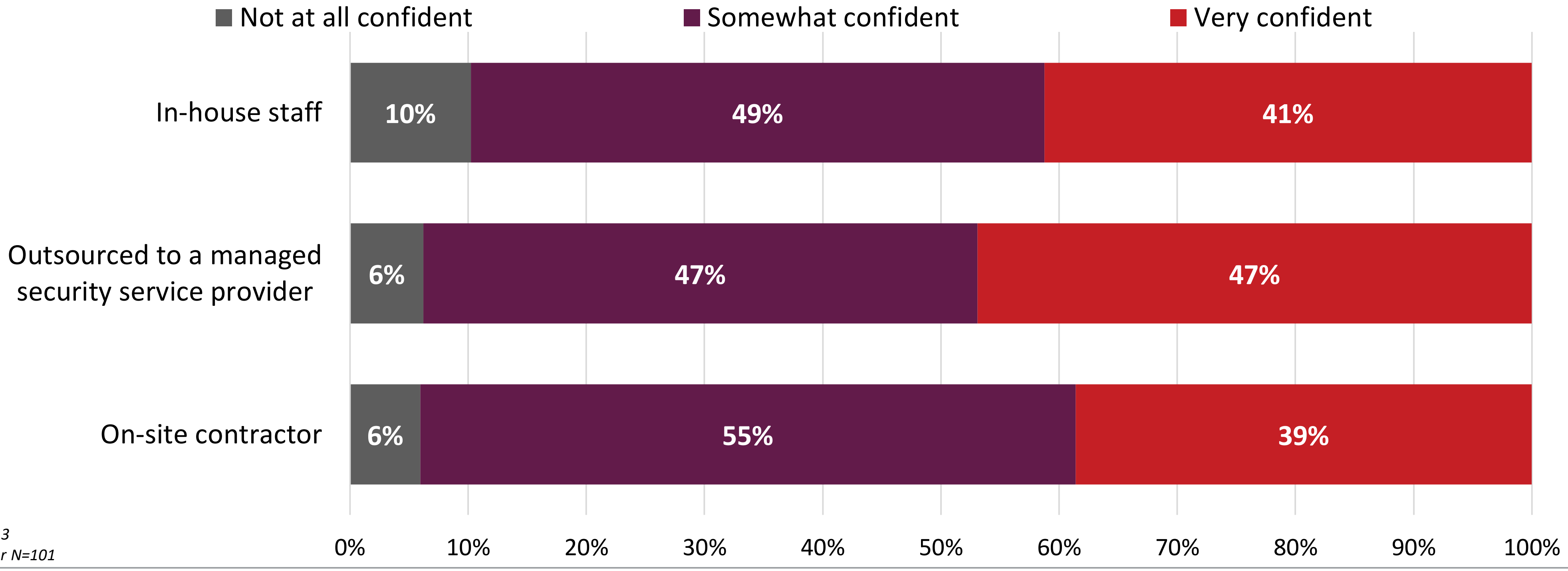
N=400
Note: Multiple responses allowed

□ = statistically significant difference

Q *How are your organization’s IT security operations currently sourced? (select all that apply)*

Confidence in Keeping Up With Threats

Only four in ten public sector respondents are very confident in their team's ability to keep up with today's evolving threats.



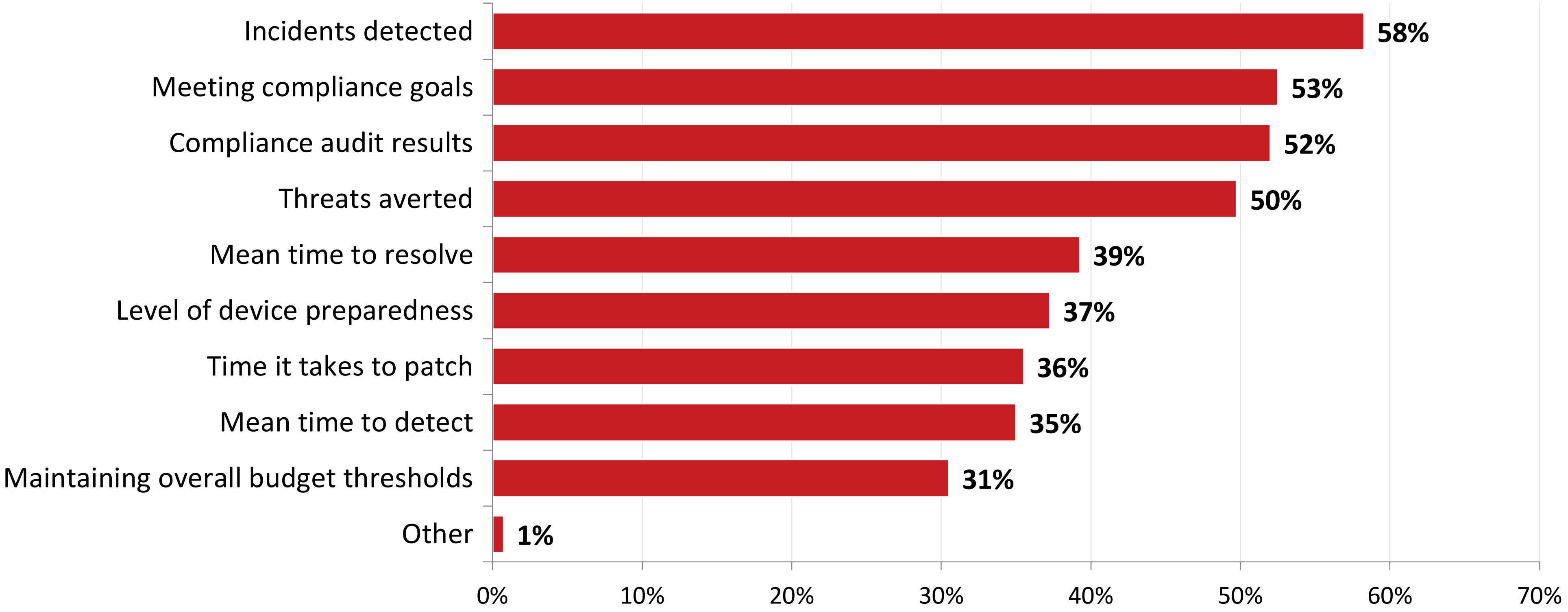
In-house N=342
Outsourced N=113
On-site contractor N=101

[IF IN-HOUSE] How confident are you that your <u>in-house staff</u> can keep up with today's evolving threats by maintaining the right skills? [IF OUTSOURCED TO A MANAGED SECURITY SERVICE PROVIDER] How confident are you that your <u>outsourced managed security service provider</u> can keep up with today's evolving threats? [IF ON-SITE CONTRACTOR] How confident are you that your <u>on-site contractor</u> can keep up with today's evolving threats?

solarwinds

Metrics Used to Measure IT Security Team Success

Incidents detected, meeting compliance goals, compliance audit results, and threats averted are the metrics used by most public sector organizations to measure the success of their organization's IT security team.



N=400
Note: Multiple responses allowed

Q *What type(s) of performance metrics does your organization use to measure the success of its IT security team? (select all that apply)*

Metrics Used to Measure Success by Organization Type

Significantly more federal than other public sector respondents indicate meeting compliance goals is used to measure the success of their organization’s IT security team.

More federal and state and local respondents than education use compliance audit results to measure success.

A significantly larger proportion of state and local respondents use threats averted.

A larger proportion of education respondents use level of device preparedness.

For incidents detected (the top metric mentioned overall), there are no significant differences between organization types.

	Federal	State & Local	Education
Meeting compliance goals	57%	53%	43%
Compliance audit results	58%	53%	39%
Threats averted	51%	56%	41%
Level of device preparedness	34%	36%	46%

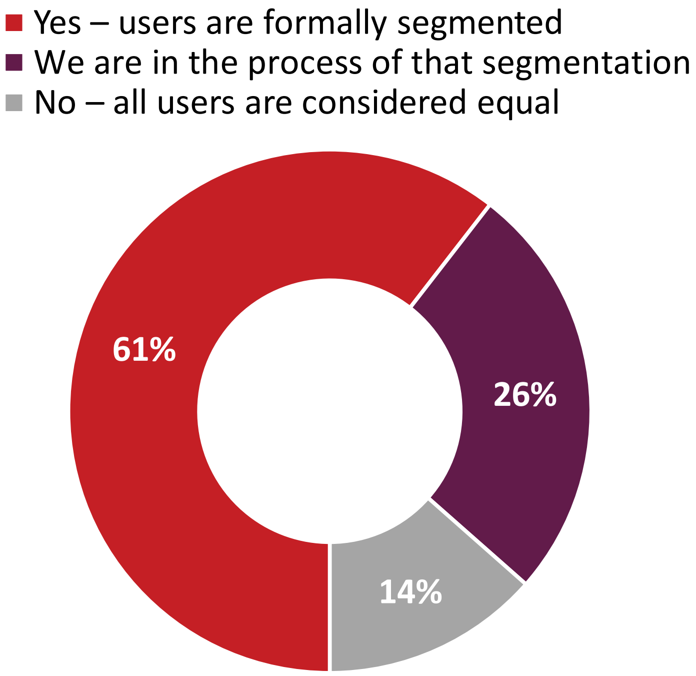
N=400
Note: Multiple responses allowed

□ = statistically significant difference

What type(s) of performance metrics does your organization use to measure the success of its IT security team? (select all that apply)

Segmenting Access by User Risk Level

Over half indicate their organization formally segments its users’ access to systems and data according to the level of risk associated with the user. Significantly more federal than other public sector respondents say their users are formally segmented.



	Federal	State & Local	Education
Yes – users are formally segmented	67%	58%	50%
We are in the process of that segmentation	21%	27%	35%

	Defense	Civilian
We are in the process of that segmentation	13%	28%

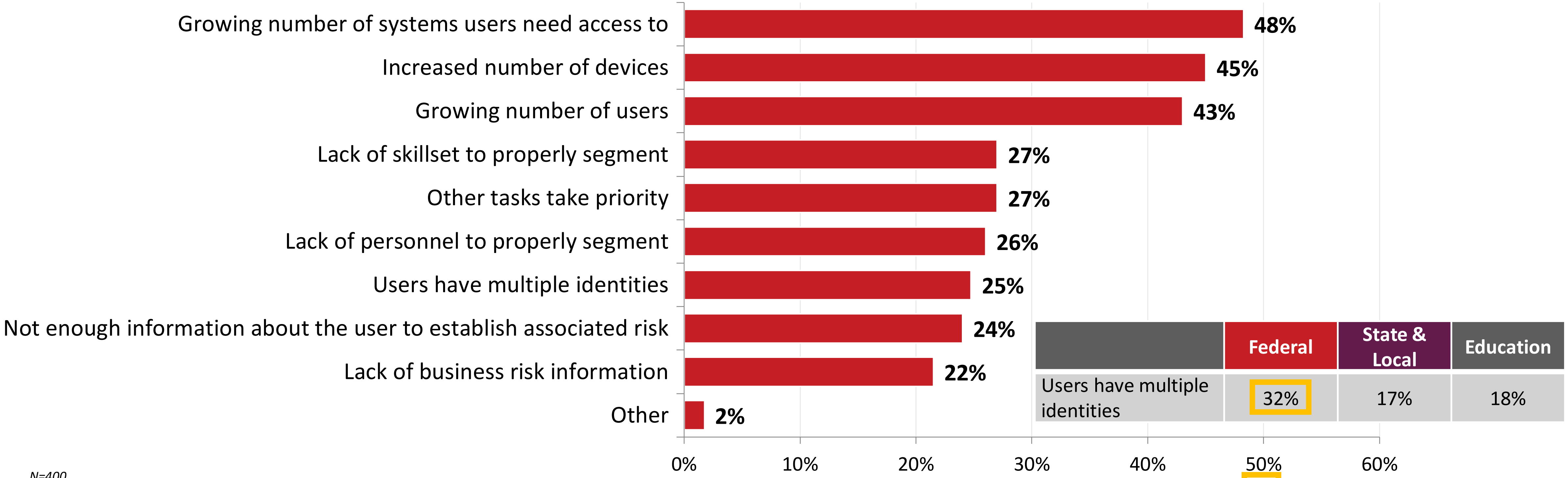
□ = statistically significant difference

N=400

Does your organization formally segment its users’ access to systems and data according to the level of risk associated with the user?

Challenges Segmenting Users by Risk Level

The growing number of systems users need access to, an increased number of devices, and a growing number of users are the top challenges public sector organizations face when segmenting users by their level of associated risk.



	Federal	State & Local	Education
Users have multiple identities	32%	17%	18%

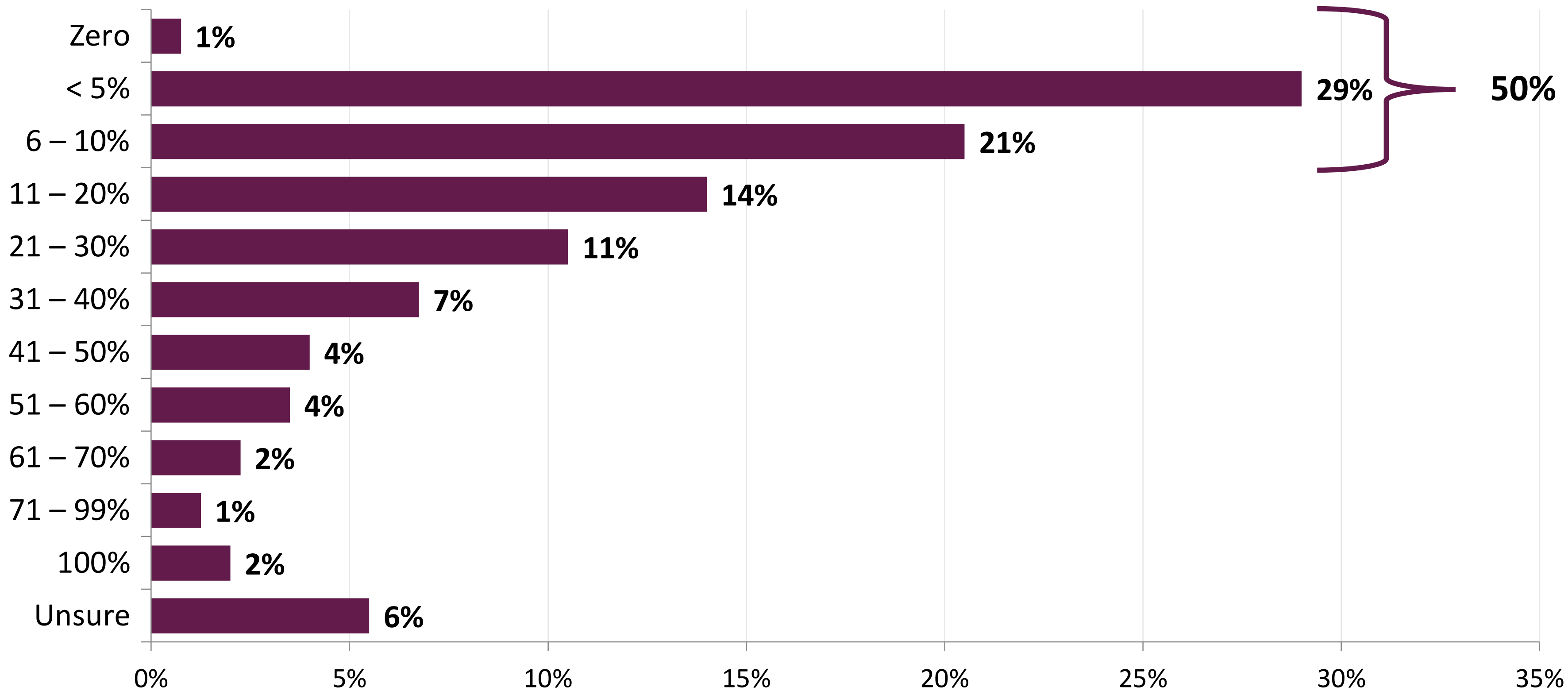
N=400
Note: Multiple responses allowed

□ = statistically significant difference

Q What challenges does your organization face when segmenting its users by their level of associated risk? (select all that apply)

Proportion of Privileged Users

The majority of respondents indicate 10 percent or less of total users at their organization are privileged users.

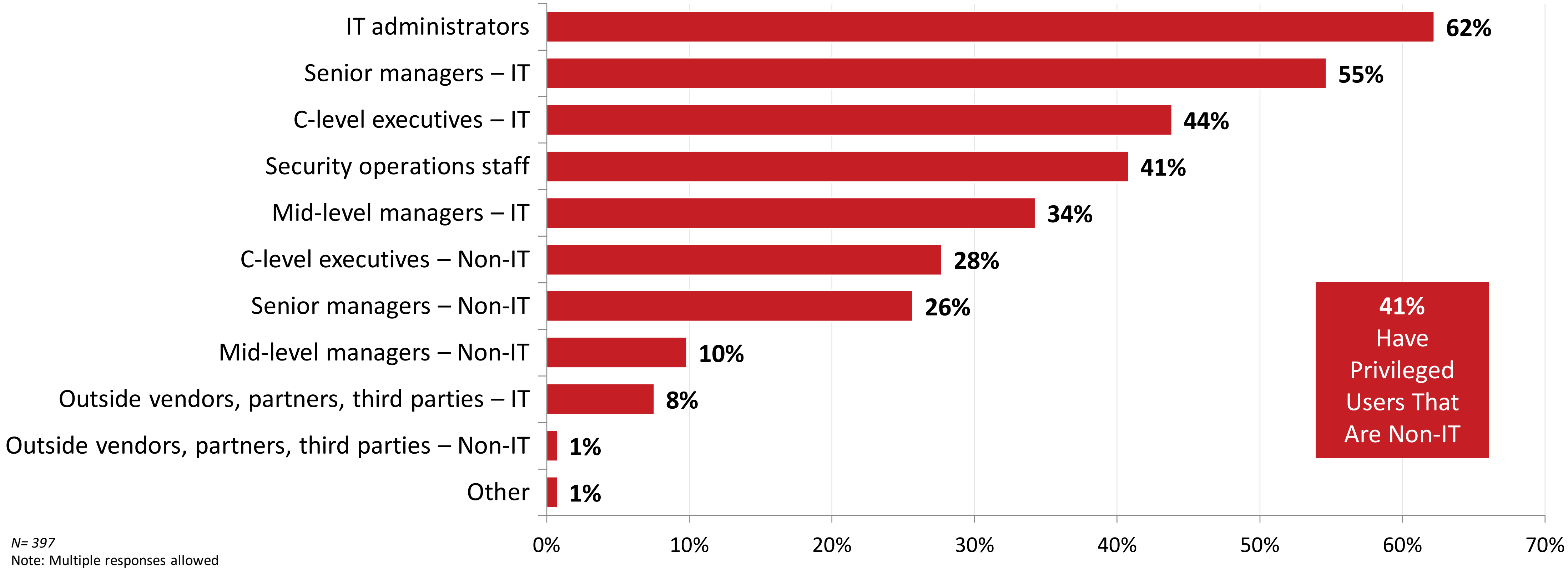


N=400

Q *What proportion of your total users at your organization are privileged users [MOUSE-OVER DEFINITION: Privileged user accounts are authorized (and therefore, trusted) to have access on an enterprise domain, allowing them to have admin rights on, for example, their local desktops or across the systems they manage.]?*

Designated Privileged Users

IT administrators are mentioned most often by respondents as being designated as privileged users at their organization.



41% Have Privileged Users That Are Non-IT

N= 397
Note: Multiple responses allowed

Who are designated as privileged users at your organization? (select all that apply)

Designated Privileged Users by Organization Type

Significantly more federal (particularly civilian) than other public sector respondents note IT administrators are designated as privileged users at their organization.

More federal and state and local (particularly state) than education respondents (driven down by K-12) indicate security operations staff are privileged users.

A larger proportion of education and state and local than federal (driven down by civilian) respondents note C-level executives – non-IT.

A larger proportion of education respondents indicate senior managers – non-IT.

More federal respondents (particularly civilian) note outside vendors, partners, third parties – IT.

	Federal	State & Local	Education
IT administrators	**68%**	62%	50%
Security operations staff	**48%**	**40%**	27%
C-level executives – Non-IT	19%	**33%**	**41%**
Senior managers – Non-IT	20%	26%	**37%**
Outside vendors, partners, third parties – IT	**13%**	4%	1%

	Defense	Civilian
IT administrators	61%	**75%**
C-level executives – Non-IT	**25%**	13%
Outside vendors, partners, third parties – IT	7%	**17%**

	State	Local
Security operations staff	**49%**	27%

	K-12	Hi-Ed
Security operations staff	16%	**38%**

□ = statistically significant difference

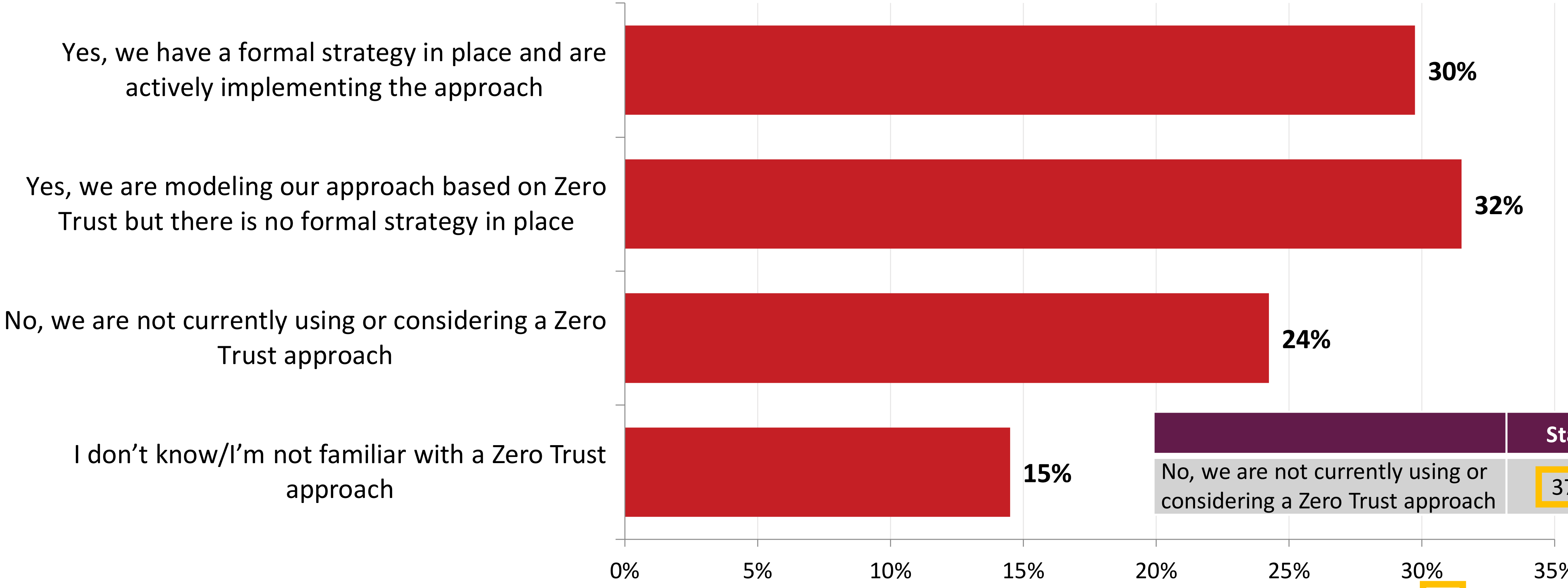
N= 397

Note: Multiple responses allowed

Who are designated as privileged users at your organization? (select all that apply)

Using a Zero-Trust Approach to IT Security

Nearly one third have a formal strategy in place and are actively implementing the Zero-Trust approach. A significantly larger proportion of state than local respondents are not using or considering a Zero-Trust approach.



	State	Local
No, we are not currently using or considering a Zero Trust approach	37%	5%

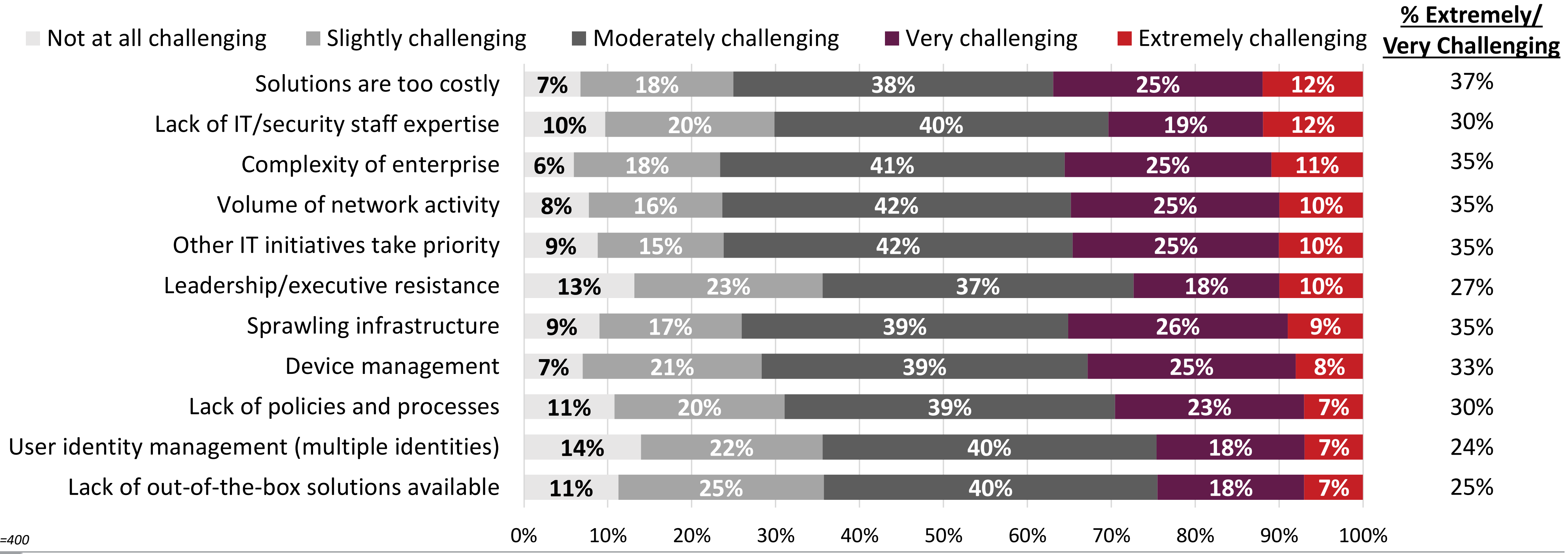
N=400

□ = statistically significant difference

Is your organization currently using or considering a Zero Trust approach to IT security? [MOUSE-OVER DEFINITION: Zero trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.]

Challenges to Adopting a Zero-Trust Approach

Solutions being too costly is the top challenge inhibiting organizations from adopting a Zero-Trust approach to IT security.



N=400

Q *To what extent are each of the following a challenge that inhibits organizations from adopting a Zero Trust [MOUSE-OVER DEFINITION: Zero trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.] approach to IT security?*

Challenges to Adopting a Zero-Trust Approach by Organization Type

Complexity of the enterprise is noted as a challenge to adopting a Zero-Trust approach to IT security significantly more often by federal than other public sector respondents.

More state than local respondents indicate complexity of the enterprise and lack of polices and processes are challenges.

More K-12 than Hi-Ed respondents indicate lack of IT/security staff expertise and leadership/executive resistance are challenges.

% Extremely/Very Challenging	Federal	State & Local	Education
Complexity of enterprise	41%	28%	32%

% Extremely/Very Challenging	State	Local
Complexity of enterprise	37%	15%
Lack of policies and processes	44%	7%

% Extremely/Very Challenging	K-12	Hi-Ed
Lack of IT/security staff expertise	37%	19%
Leadership/executive resistance	37%	15%

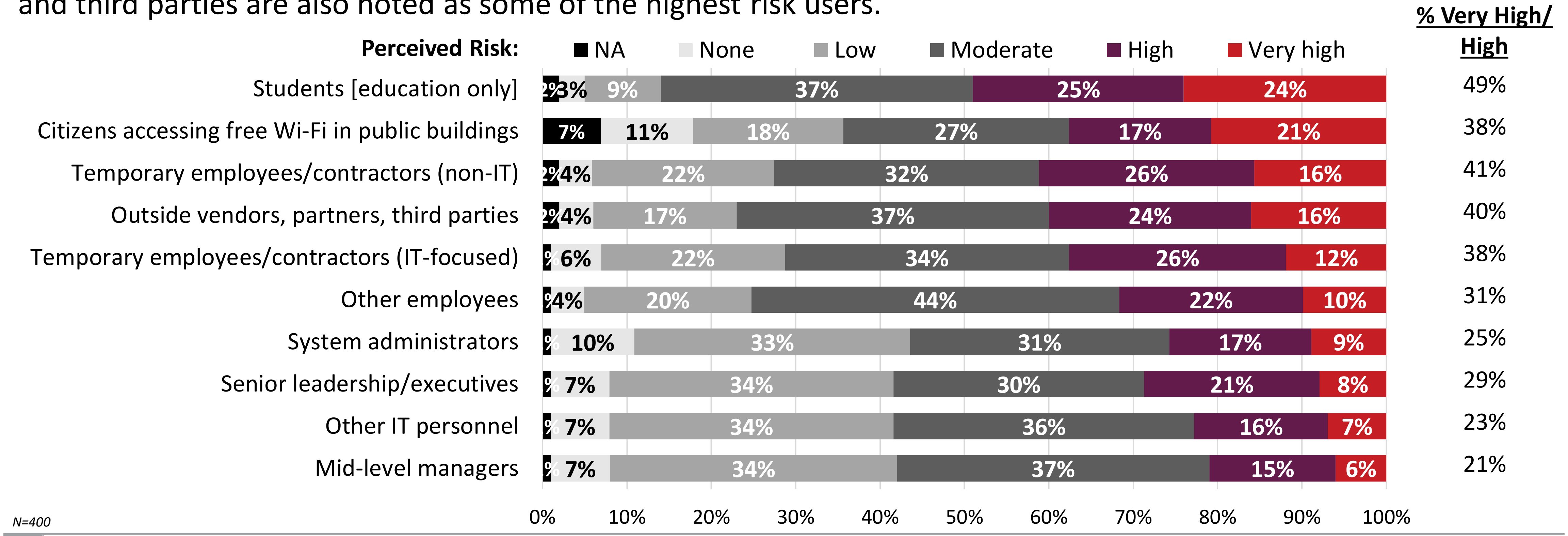
□ = statistically significant difference

N=400

Q *To what extent are each of the following a challenge that inhibits organizations from adopting a Zero Trust [MOUSE-OVER DEFINITION: Zero trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.] approach to IT security?*

Risk Associated With User Types

Although only rated by education respondents, students are the highest risk to IT security. Overall, citizens accessing free Wi-Fi in public buildings, temporary employees/contractors (non-IT), and outside vendors, partners, and third parties are also noted as some of the highest risk users.



N=400

How would you rate the perceived risk associated with the following types of users as it pertains to IT security, access rights and the potential threat?

Risk Associated With User Types by Organization Type

Federal respondents rate the perceived risk associated with temporary employees/contractors (both non-IT and IT-focused) and outside vendors, partners, and third parties higher than other public sector respondents' ratings.

Four in ten federal and state and local government respondents note temporary employees/contractors and outside vendors, partners, and third parties as the greatest risks to security.

Education respondents rate citizens accessing free Wi-Fi in public buildings riskier than other public sector respondents' ratings.

More state than local respondents find temporary employees/contractors (both non-IT and IT-focused) and outside vendors, partners, and third parties risky.

% Very High/High	Federal	State & Local	Education
Temporary employees/contractors (non-IT)	45%	41%	33%
Temporary employees/contractors (IT-focused)	45%	38%	25%
Outside vendors, partners, third parties	47%	40%	28%
Citizens accessing free Wi-Fi in public buildings	36%	31%	49%

% Very High/High	State	Local
Temporary employees/contractors (non-IT)	53%	24%
Temporary employees/contractors (IT-focused)	54%	15%
Outside vendors, partners, third parties	51%	24%

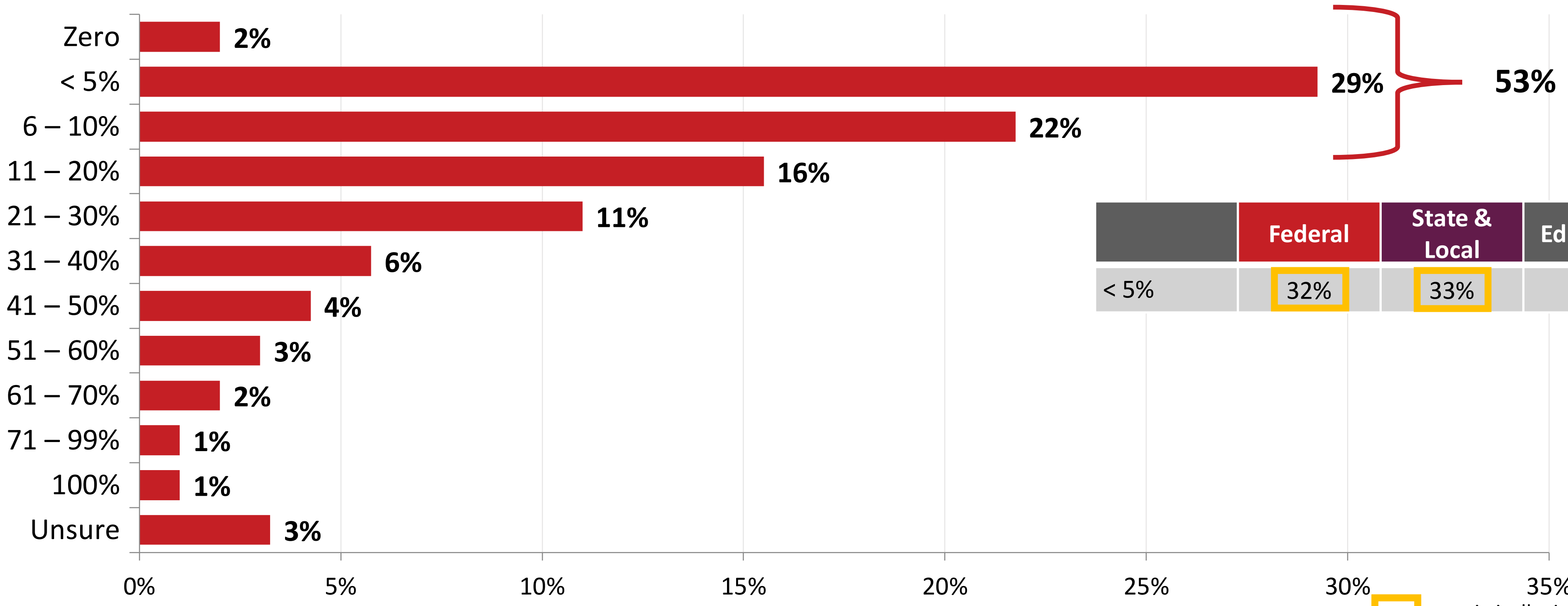
□ = statistically significant difference

N=400

How would you rate the perceived risk associated with the following types of users as it pertains to IT security, access rights and the potential threat?

Users Most at Risk for Doing Harm

The majority estimate 10 percent or less of their organization's users are most at risk for potentially doing harm (either careless or malicious) to their organization.



	Federal	State & Local	Education
< 5%	32%	33%	20%

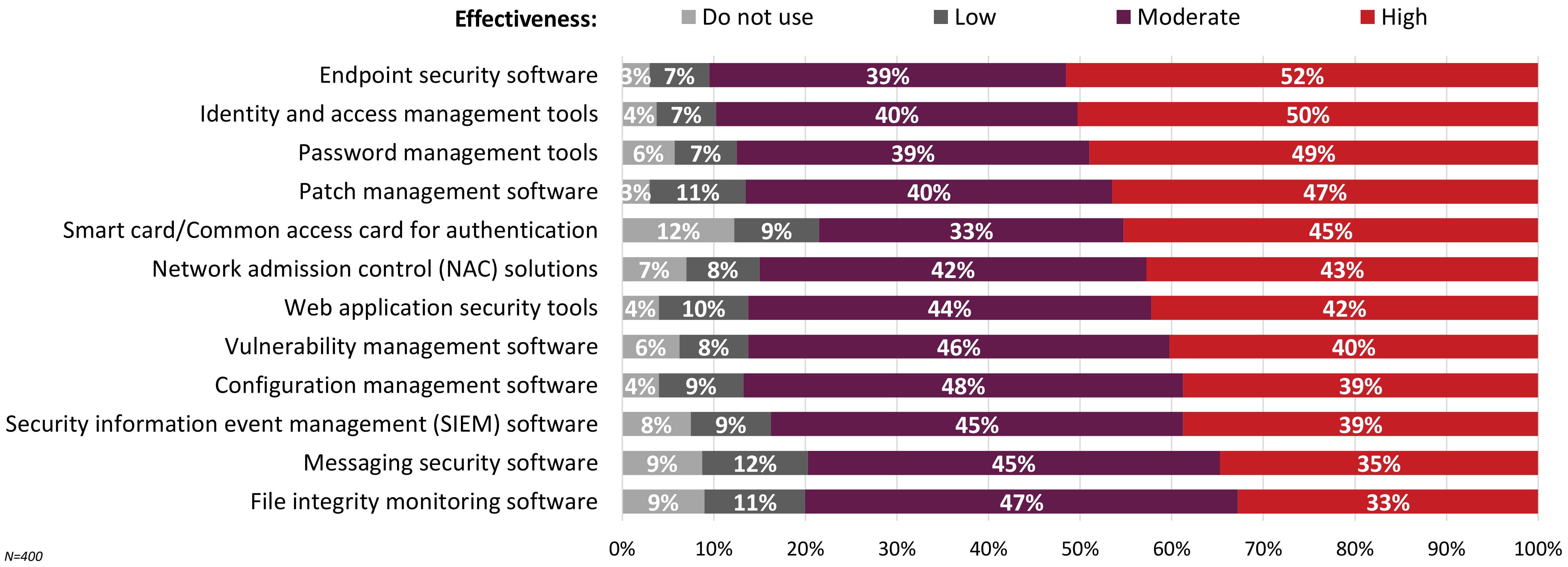
N=400

□ = statistically significant difference

What percent of your organization's users do you estimate to be most at risk for potentially doing harm (either careless or malicious) to your organization?

Effectiveness of Tools to Foster Security

Endpoint security software is the highest rated tool for effectively fostering network and application security.



N=400

The following are tools and practices that foster network and application security. Please indicate the effectiveness for each at your organization.

Effectiveness of Tools by Organization Type

More federal than other respondents indicate endpoint security software, identity and access management tools, patch management software, smart cards, and network admissions control solutions are highly effective at fostering network and application security at their organization.

A larger proportion of defense than civilian respondents indicate NAC solutions are highly effective.

More state than local respondents indicate identity and access management tools and smart cards/common access cards for authentication are effective.

A larger proportion of Hi-Ed than K-12 respondents indicate messaging security software is effective.

% High	Federal	State & Local	Education
Endpoint security software	57%	41%	51%
Identity and access management tools	56%	42%	48%
Patch management software	51%	48%	37%
Smart card/Common access card for authentication	65%	30%	21%
Network admission control (NAC) solutions	49%	35%	39%

% High	Defense	Civilian
Network admission control (NAC) solutions	56%	42%

% High	State	Local
Identity and access management tools	53%	27%
Smart card/Common access card for authentication	39%	17%

% High	K-12	Hi-Ed
Messaging security software	21%	46%

□ = statistically significant difference

N=400

The following are tools and practices that foster network and application security. Please indicate the effectiveness for each at your organization.

Examples of Comments

A major ongoing challenge is integrating security protocols without detriment to network latency and response times.

IT AND NETWORK SYSTEMS OPERATIONS MANAGER, DEFENSE

Because it is the government sector and government contracts are at play. I think that there is a ceiling when it comes to looking at innovative, out-of-the-box alternatives.

SYSTEMS ADMINISTRATOR, FEDERAL CIVILIAN

Security is everyone's job, but holding the team accountable is lacking. Until there are real individual accountability regimens in place, the network will remain at risk.

DIVISION CHIEF, FEDERAL CIVILIAN

Meeting the online needs of 12,000 plus students always presents challenging security issues, but we have been able to manage without a major event so far.

VP OPERATIONS, HI-ED

Unfortunately, budget constraints and operational red tape prevents things from being as secure and efficient as they need to be.

IT MANAGER, K-12

Not enough manpower, money, or resources. Waiting for a ticking bomb to go off.

CTO, K-12

Greatest challenge is always protecting data from malware and attacks from both internal and external users.

DIRECTOR, STATE GOV

Everything starts at the top. If C-level doesn't put an emphasis on security, it puts us at risk.

IT MANAGER, LOCAL GOV

Our organization operates in denial with a preference for reactionary behavior instead of operating proactively. Government agencies tend to view IT spending as throwing money into a black hole until something occurs.

SR. IT PROJECT MANAGER AND ANALYST, STATE GOV

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

Key Takeaways

The federal audience tends to be more mature than state and local and education audiences in its IT security capabilities.

- Federal respondents’ ratings are significantly more mature than state and local and education respondents in many cybersecurity capabilities. State respondents also tend to be more mature in their capabilities than local respondents, and Hi-Ed respondents are more mature than K-12.
- Significantly more federal than other public sector respondents think compliance mandates or regulations and investment in training for employees have impacted their organization’s evolution of its IT security policies and practices.
- More federal than other public sector respondents say their users’ access to systems and data are formally segmented according to the level of risk associated with the user.
- More federal than other public sector respondents indicate endpoint security software, identity and access management tools, patch management software, smart cards, and network admissions control solutions are highly effective at fostering network and application security at their organization.

Key Takeaways

Budget constraints is the most significant high-level obstacle to maintaining or improving IT security in public sector organizations.

- Budget constraints top the list of significant obstacles to maintaining or improving organization IT security for all public sector groups, and significantly more so for education respondents (driven by K-12).
- Budget constraints have declined since 2014 for the federal audience, but still remain the top obstacle.
- Solutions being too costly is the top challenge that inhibits organizations from adopting a Zero-Trust approach to IT security.

Key Takeaways

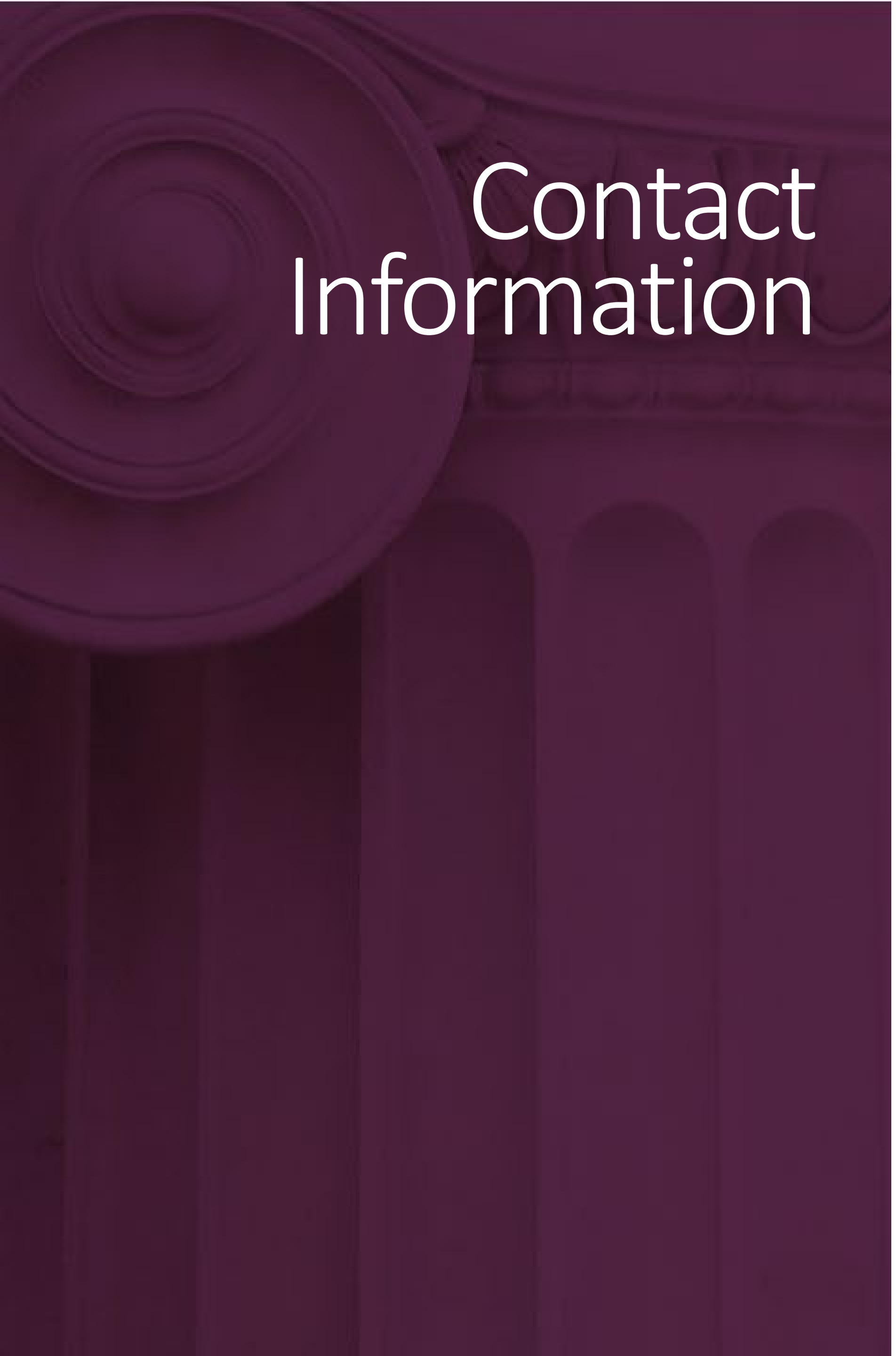
Complexity of the environment is one of the top challenges to improving IT security, adopting a Zero-Trust approach, and user segmentation.

- Complexity of the internal environment is the second most significant high-level obstacle to maintaining or improving IT security. Federal respondents indicate the complexity of the internal environment more than other public sector respondents do. The complexity of the internal environment as an obstacle has increased since 2014 for the federal audience.
- Complexity of the enterprise is one of the top challenges that inhibit organizations from adopting a Zero-Trust approach to IT security.
- The growing number of systems users need access to, an increased number of devices, and a growing number of users are the top challenges organizations face when segmenting users by their level of associated risk.

Key Takeaways

The majority note careless/ untrained insiders as the greatest source of IT security threats at their organization. But overall, most feel their organization is keeping up with threats.

- Over half note careless/untrained insiders as the largest source of security threats.
- Students, citizens accessing free Wi-Fi in public buildings, temporary employees/contractors (non-IT), and outside vendors, partners, and third parties are noted as some of the highest risk users to IT security.
- The majority estimate 10 percent or less of their organization's users are most at risk for potentially doing harm (either careless or malicious) to their organization.
- Regardless of the method being used to source their organization's IT security operations (in-house staff, outsourced to a managed security service provider, or on-site contractor), most are confident they are keeping up with today's evolving threats.



Contact Information

Elizabeth Lowery, Research Manager, Market Connections, Inc.

ElizabethL@marketconnectionsinc.com
703-972-5875

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

LaurieM@marketconnectionsinc.com
571-257-3845

Lisa M. Sherwin Wulf, Vice President of Americas Marketing – ITOM, SolarWinds

Lisa.SherwinWulf@solarwinds.com
703-386-2628
www.solarwinds.com/government
LinkedIn: SolarWinds Government

solarwinds government

Market Connections®
Research you can act on.