solarwinds

Market Connections
Research you can act on.

SolarWinds®
Federal Cybersecurity Survey
Summary Report

March 26, 2014

Background and Approach

SolarWinds and Market Connections worked together to design and conduct a blind online cybersecurity survey among 200 federal government IT decision makers and influencers in January and February 2014.

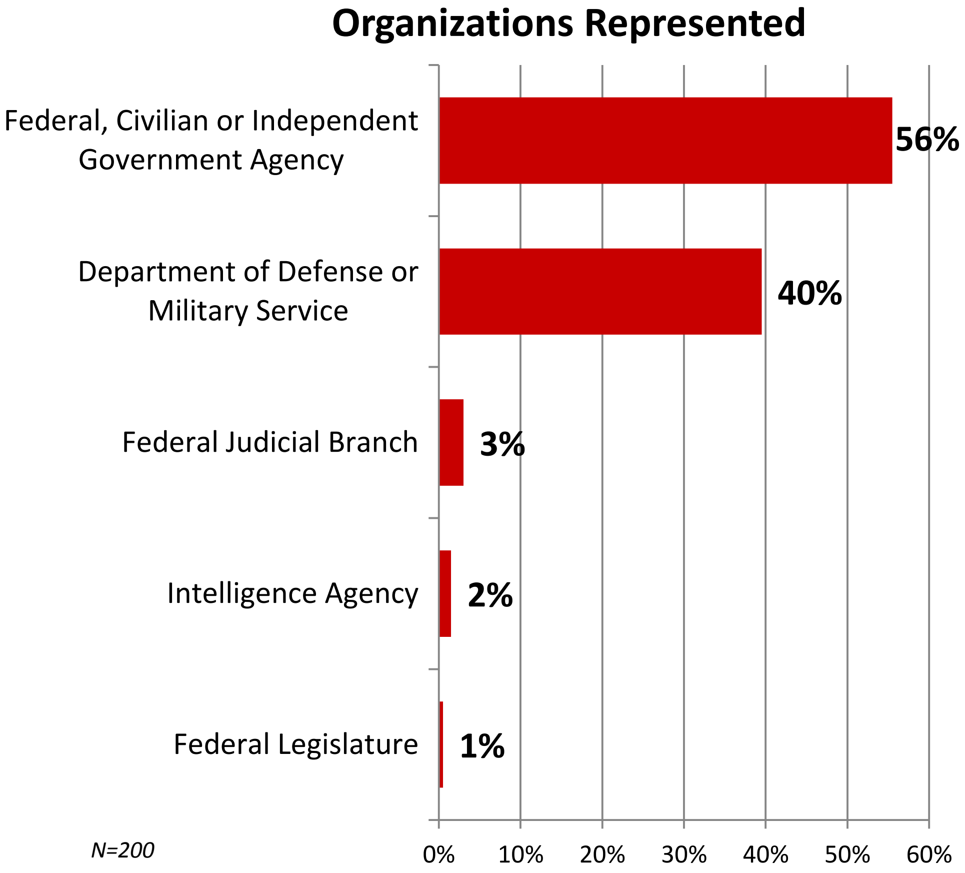
Throughout the report, notable significant differences are reported.

- Statistical analyses were conducted for continuous monitoring status, agency type and job function. There were no significant differences detected by job function.

Due to rounding, graphs may not add up to 100%.

Organizations Represented

- If a respondent did not work for any of the specific organization types noted below, the survey was terminated.

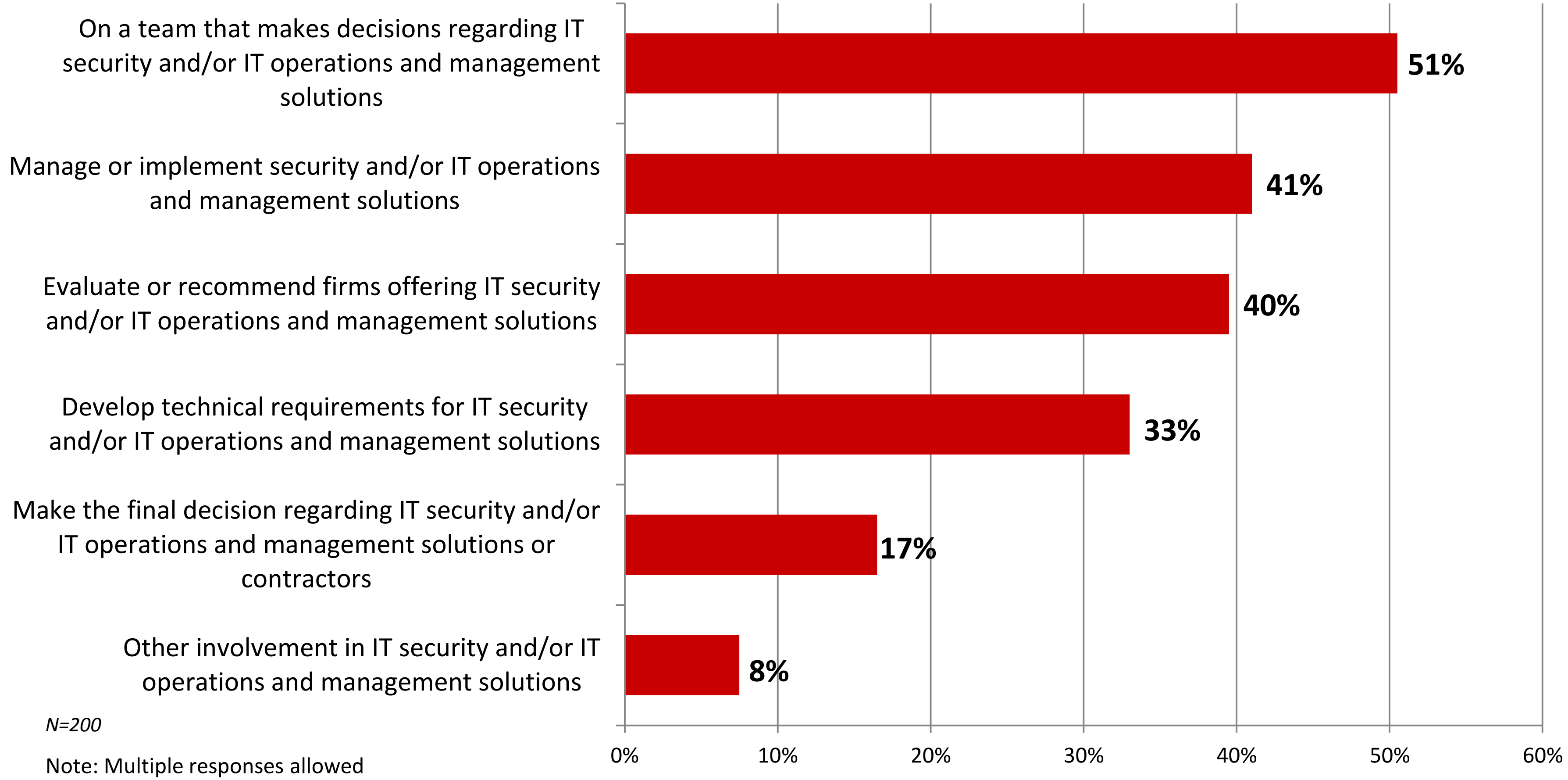


Sample Organizations Represented (In Alphabetical Order)	
Air Force	Department of Transportation (DOT)
Army	Department of Treasury (TREAS)
Department of Agriculture (USDA)	Department of Veteran Affairs (VA)
Department of Commerce (DOC)	Federal Aviation Administration (FAA)
Department of Defense (DOD)	Judicial/Courts
Department of Energy (DOE)	Marine Corps
Department of Homeland Security (DHS)	National Aeronautics and Space Administration (NASA)
Department of Labor (DOL)	Navy
Department of State (DOS)	Social Security Administration (SSA)
Department of the Interior (DOI)	US Postal Service (USPS)

Q *Which of the following best describes your current employer?*
What agency do you work for?

Decision Making Involvement

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



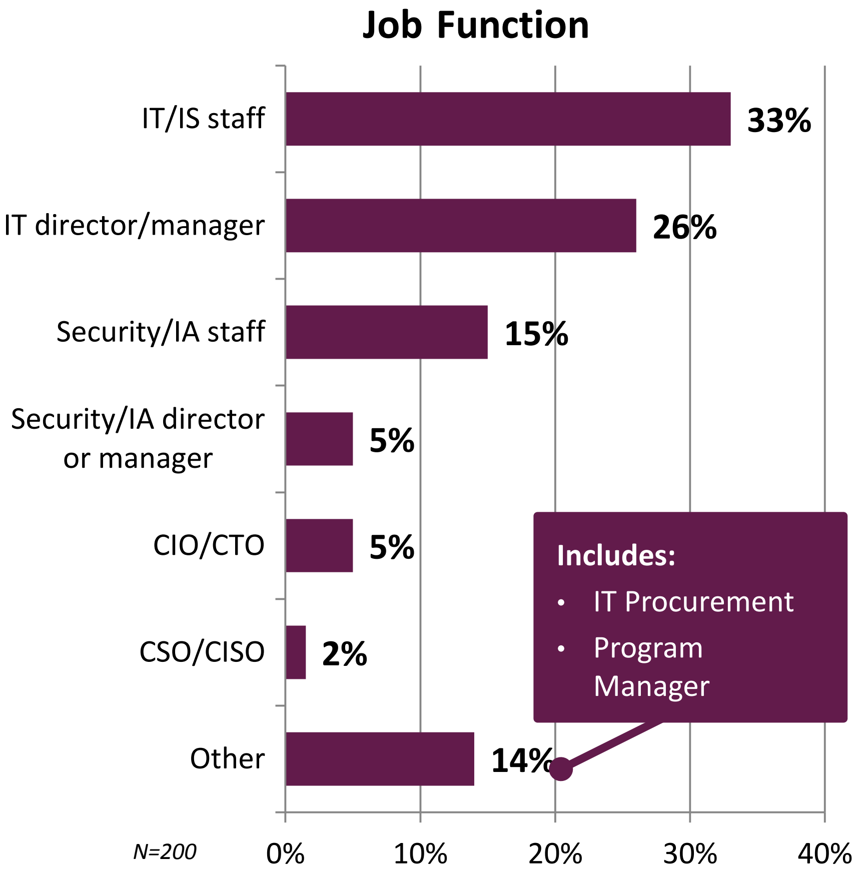
N=200

Note: Multiple responses allowed

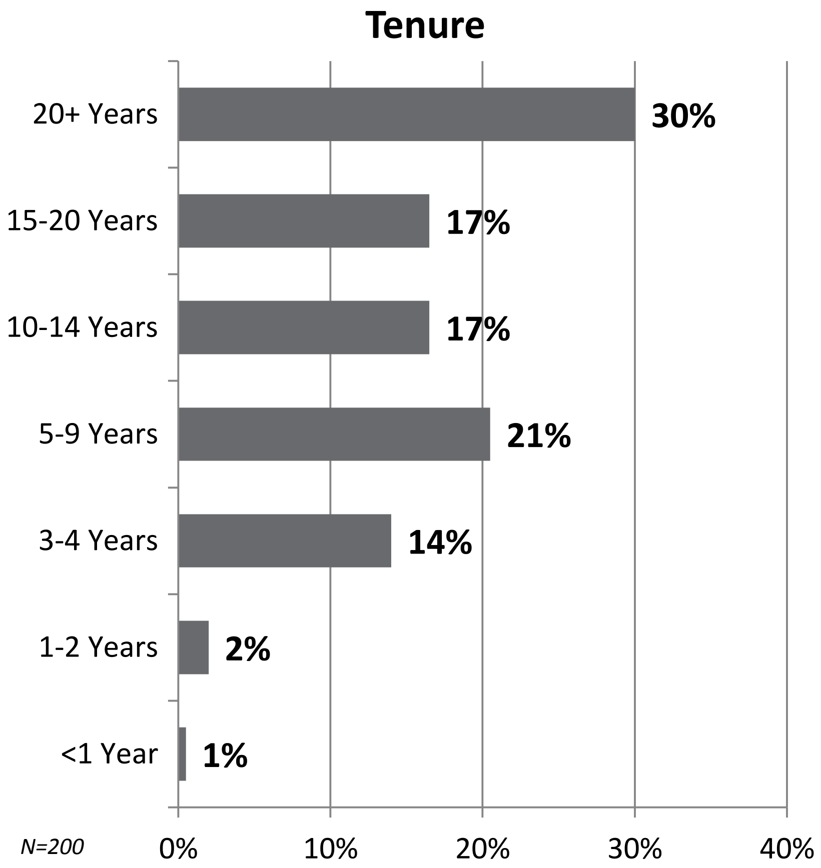
Q *How are you involved in your organization's decisions or recommendations regarding IT operations and management and IT security solutions and services? (select all that apply)*

Job Function and Tenure

- A variety of job functions and tenures are represented in the sample, with most being IT/IS staff and working at their agency for over 20 years.



Includes:
- IT Procurement
- Program Manager

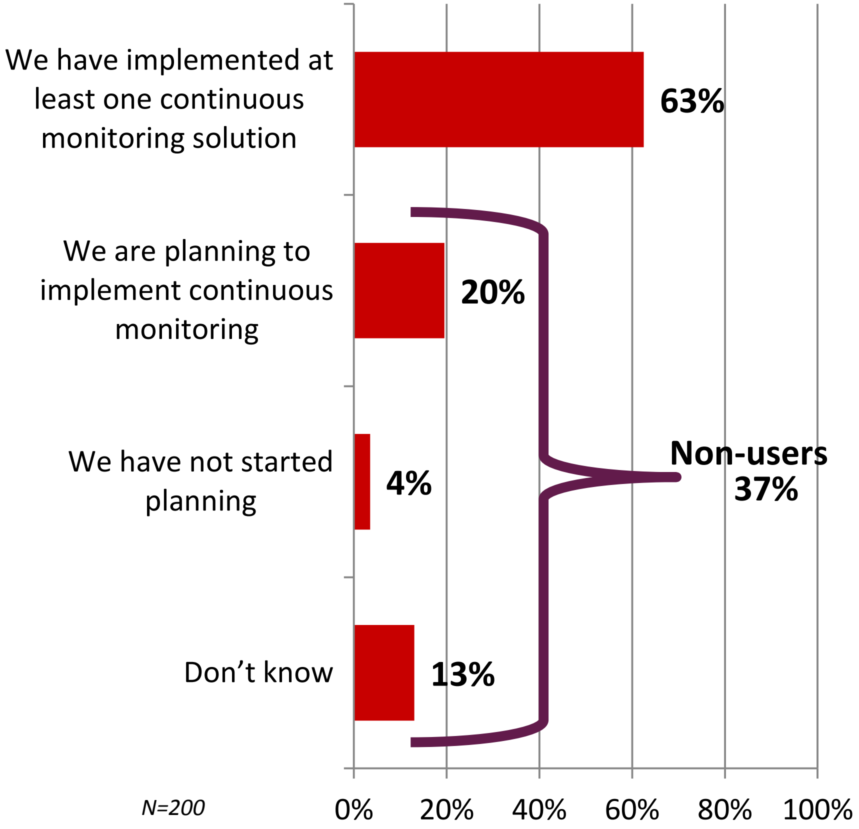


Q *Which of the following best describes your current job title/function?*
How long have you been working at your current agency?

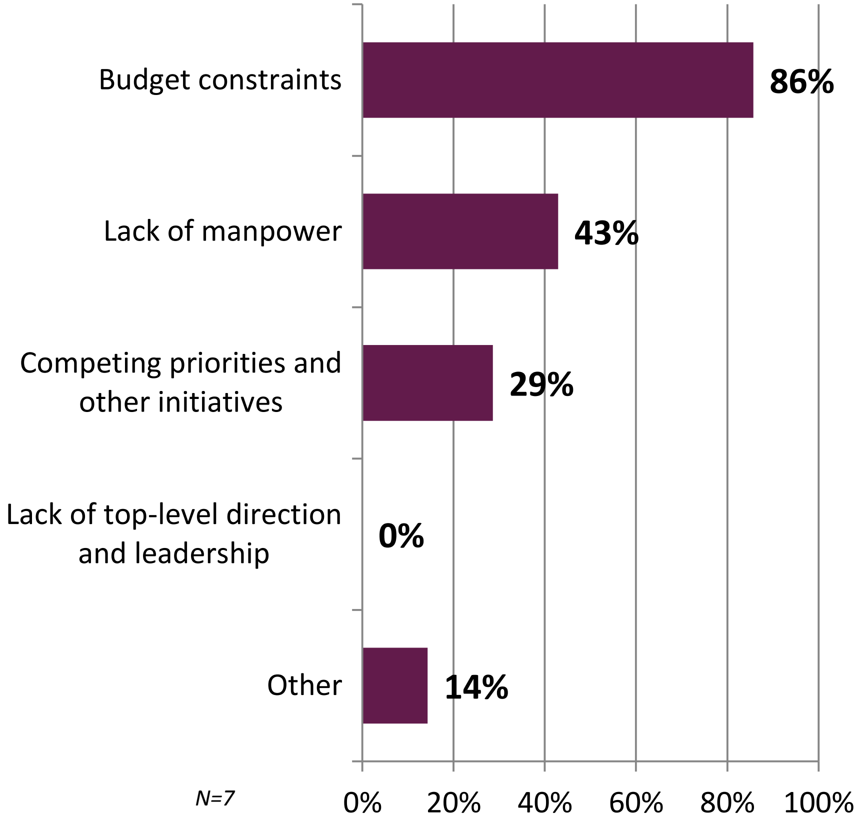
Continuous Monitoring Plan

- Two-thirds report having implemented at least one continuous monitoring solution.
- The majority of those who have not started planning report it is due to budget constraints.

Supporting Requirements



Reasons for Not Planning

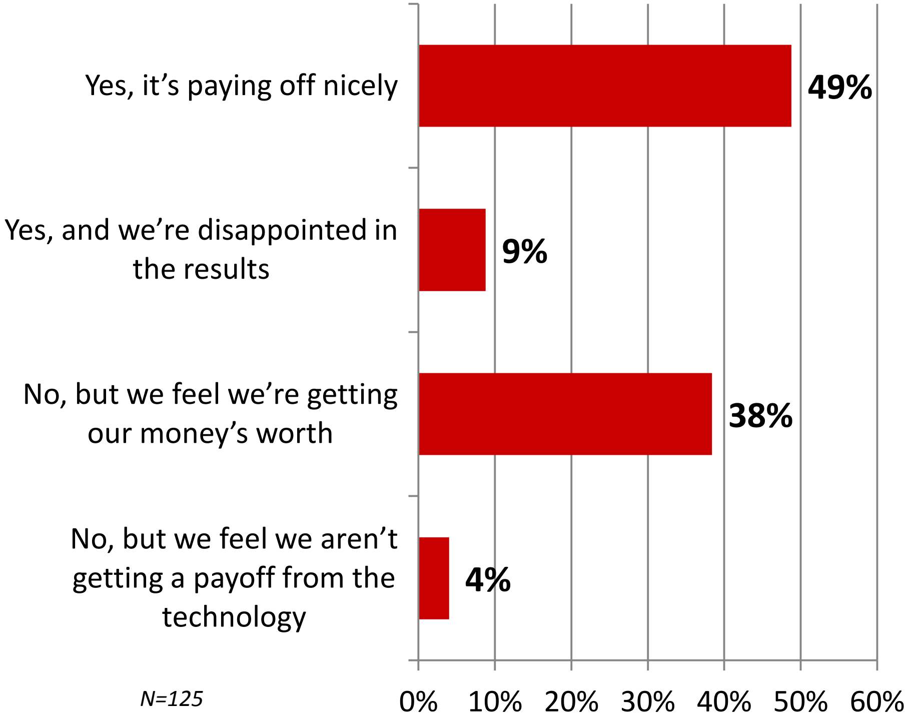


Q *How well equipped is your agency to support federal government (ex. OMB mandate, DISA STIG, etc.) continuous monitoring requirements?*
What are the reasons that you have not started planning to implement continuous monitoring? (select all that apply)

Return on Investment

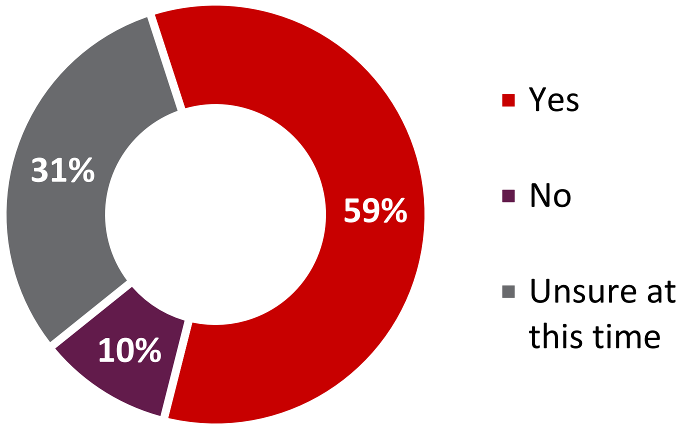
- Nearly half of respondents have measured the return on investment of continuous monitoring and report it is paying off nicely.
- Of those planning to implement continuous monitoring, the majority plan to measure its return on investment once implemented.

Have Measured Return on Investment



N=125

Plan to Measure ROI Once Implemented

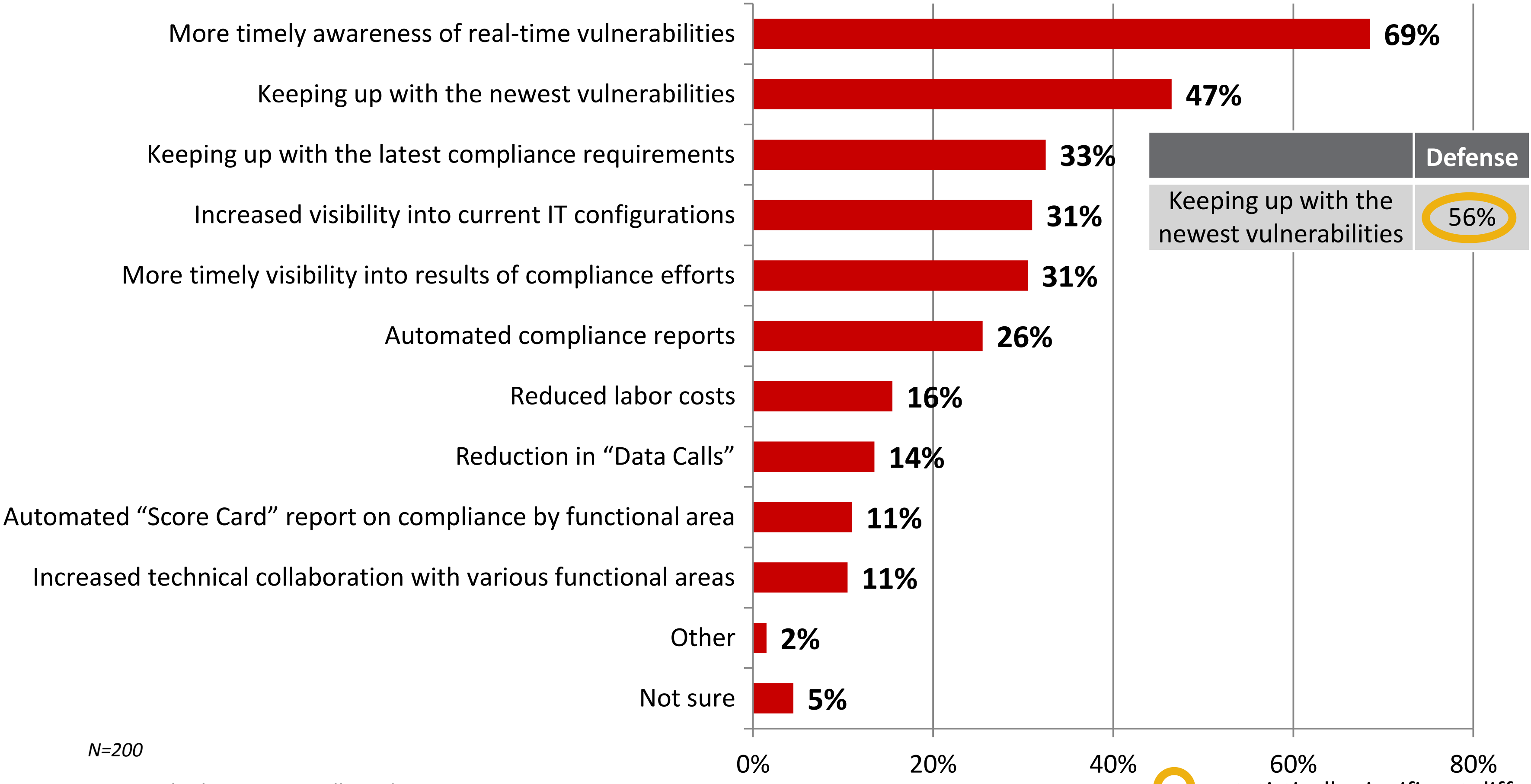


N=39

Q *Have you measured the return on your investment in using continuous monitoring?*
Once implemented, do you plan to measure the return on your investment in using continuous monitoring?

Continuous Monitoring Benefits

- The majority perceive more timely awareness of real-time vulnerabilities as the top benefit to comprehensive continuous monitoring.



	Defense	Civilian
Keeping up with the newest vulnerabilities	56%	40%

N=200

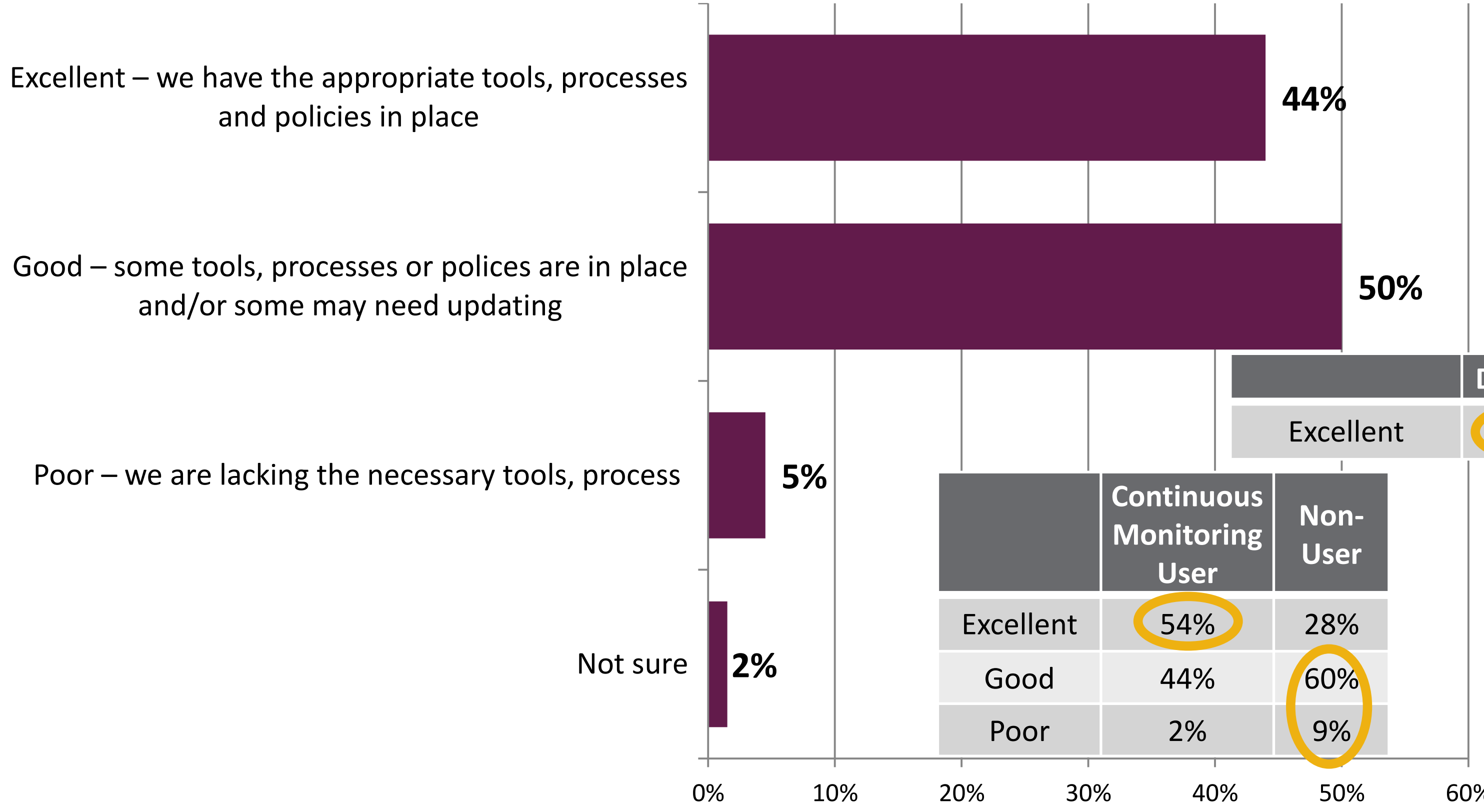
Note: Multiple responses allowed

○ = statistically significant difference

Q *What do you perceive as the top three benefits to comprehensive continuous monitoring? (select three)*

Cybersecurity Readiness

- The majority describe their agency's overall cybersecurity readiness as good or excellent. A significantly greater proportion of defense agency respondents as well as respondents that use continuous monitoring rate their readiness as excellent.



	Defense	Civilian
Excellent	54%	37%

	Continuous Monitoring User	Non-User
Excellent	54%	28%
Good	44%	60%
Poor	2%	9%

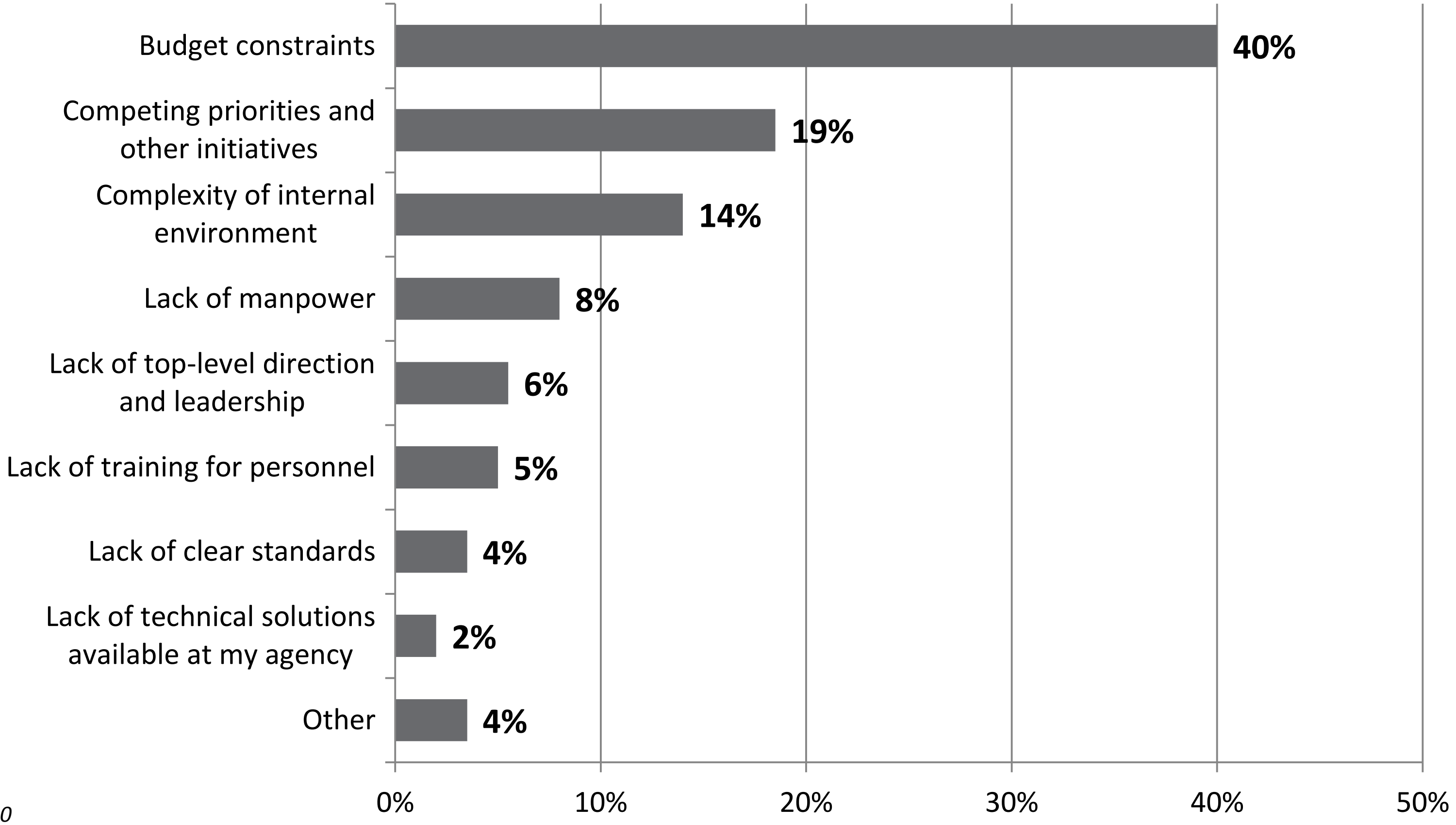
N=200

○ = statistically significant difference

Q *How would you describe your agency's overall cybersecurity readiness?*

IT Security Obstacles

- Respondents most often consider budget constraints as the single most significant high-level obstacle to maintain or improve IT security.

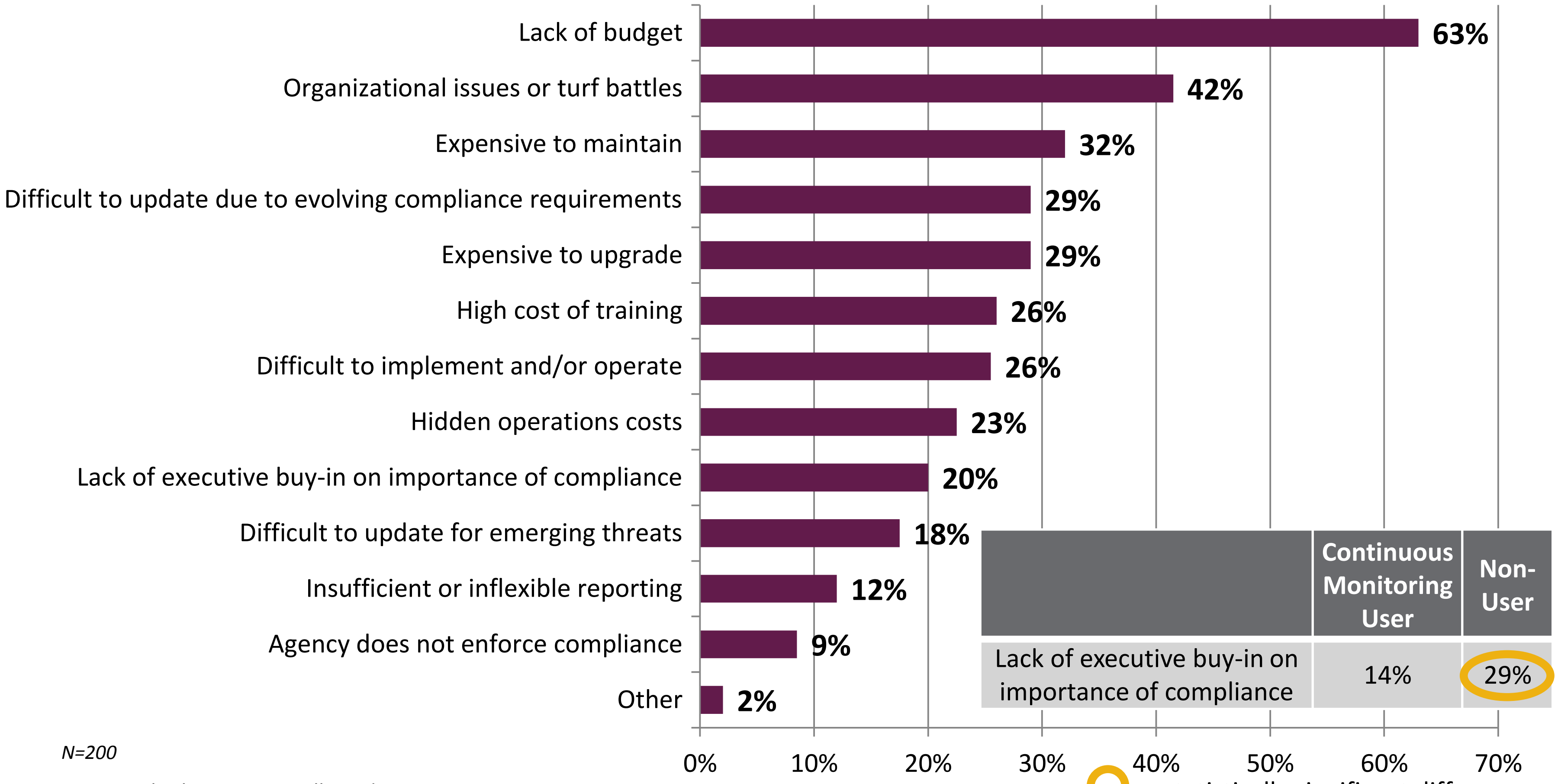


N=200

Q *What is the single most significant high-level obstacle to maintain or improve IT security at your agency?*

Tool Implementation Frustrations

- The majority report lack of budget is the biggest frustration an IT manager faces in implementing cyber security tools.



	Continuous Monitoring User	Non-User
Lack of executive buy-in on importance of compliance	14%	29%

N=200

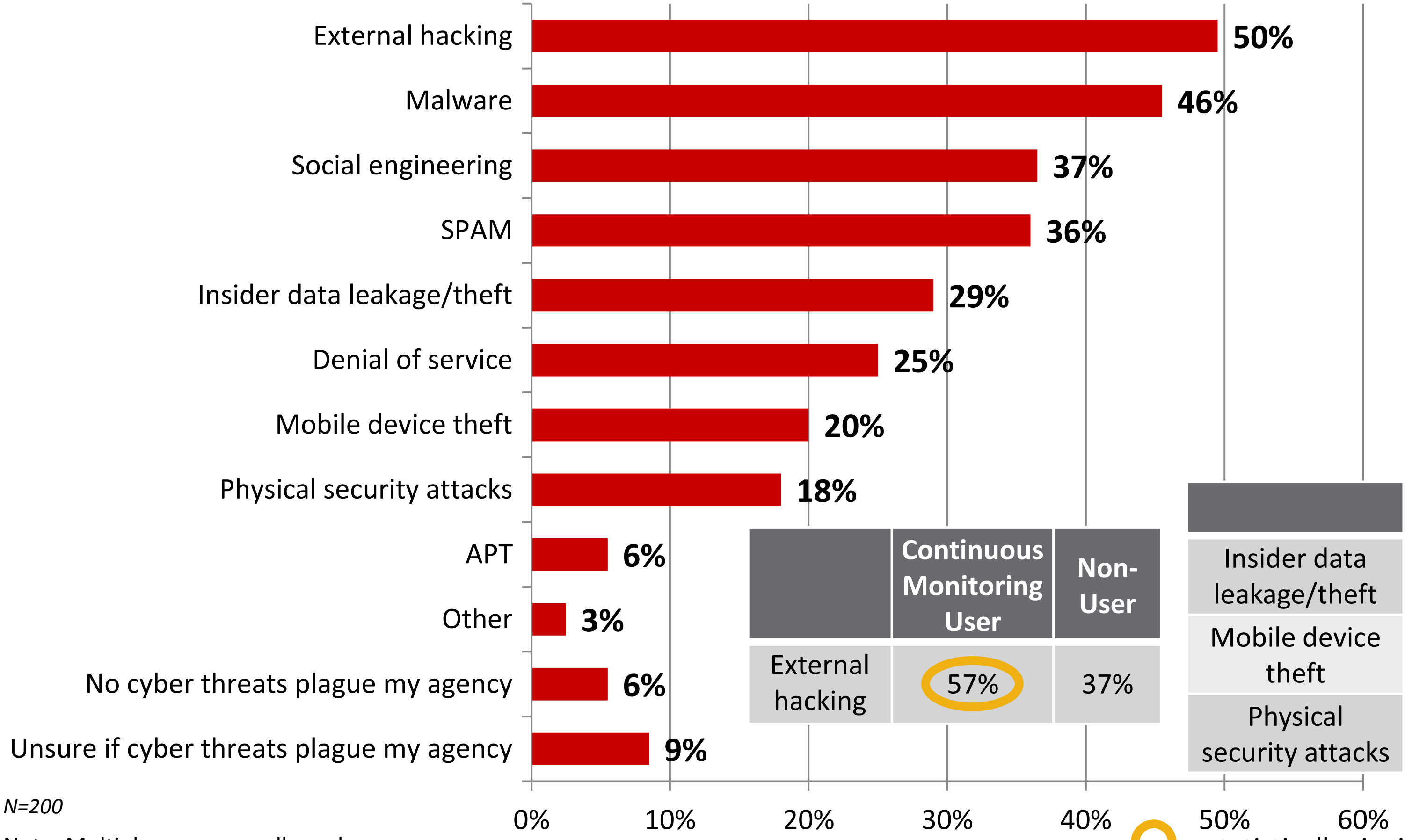
Note: Multiple responses allowed

○ = statistically significant difference

Q *What are the biggest frustrations an IT manager in your agency faces in implementing cyber security tools? (select all that apply)*

Cybersecurity Threats

- External hacking and malware are the overall top cybersecurity threats plaguing agencies.



	Continuous Monitoring User	Non-User
External hacking	57%	37%

	Defense	Civilian
Insider data leakage/theft	41%	21%
Mobile device theft	12%	25%
Physical security attacks	25%	13%

N=200

Note: Multiple responses allowed

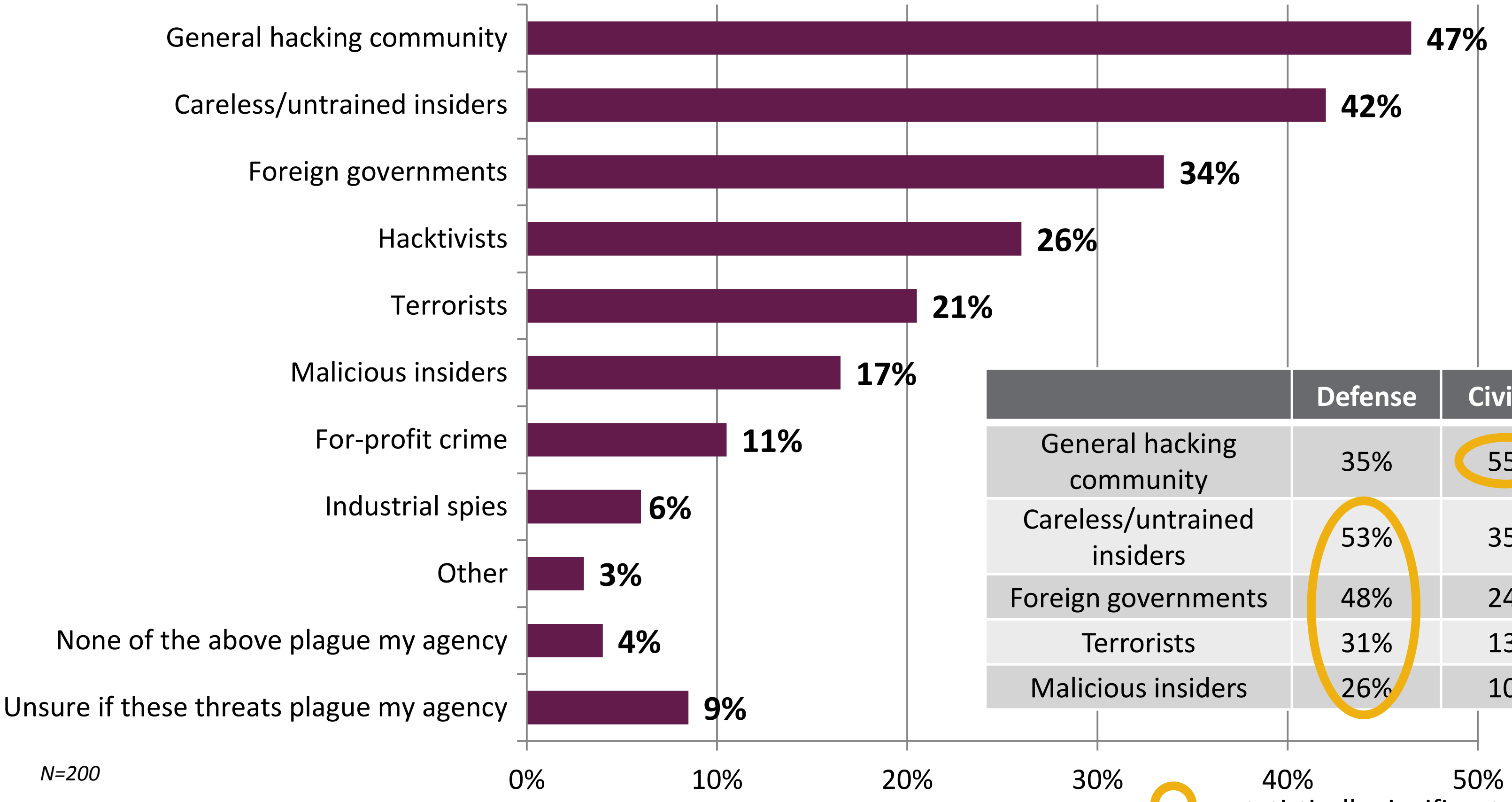
○ = statistically significant difference

Q *What types of cybersecurity threats are plaguing your agency? (select all that apply)*

Security Threat Sources

solarwinds

- The general hacking community and careless/untrained insiders are the largest sources of security threats at agencies.



	Defense	Civilian
General hacking community	35%	55%
Careless/untrained insiders	53%	35%
Foreign governments	48%	24%
Terrorists	31%	13%
Malicious insiders	26%	10%

N=200

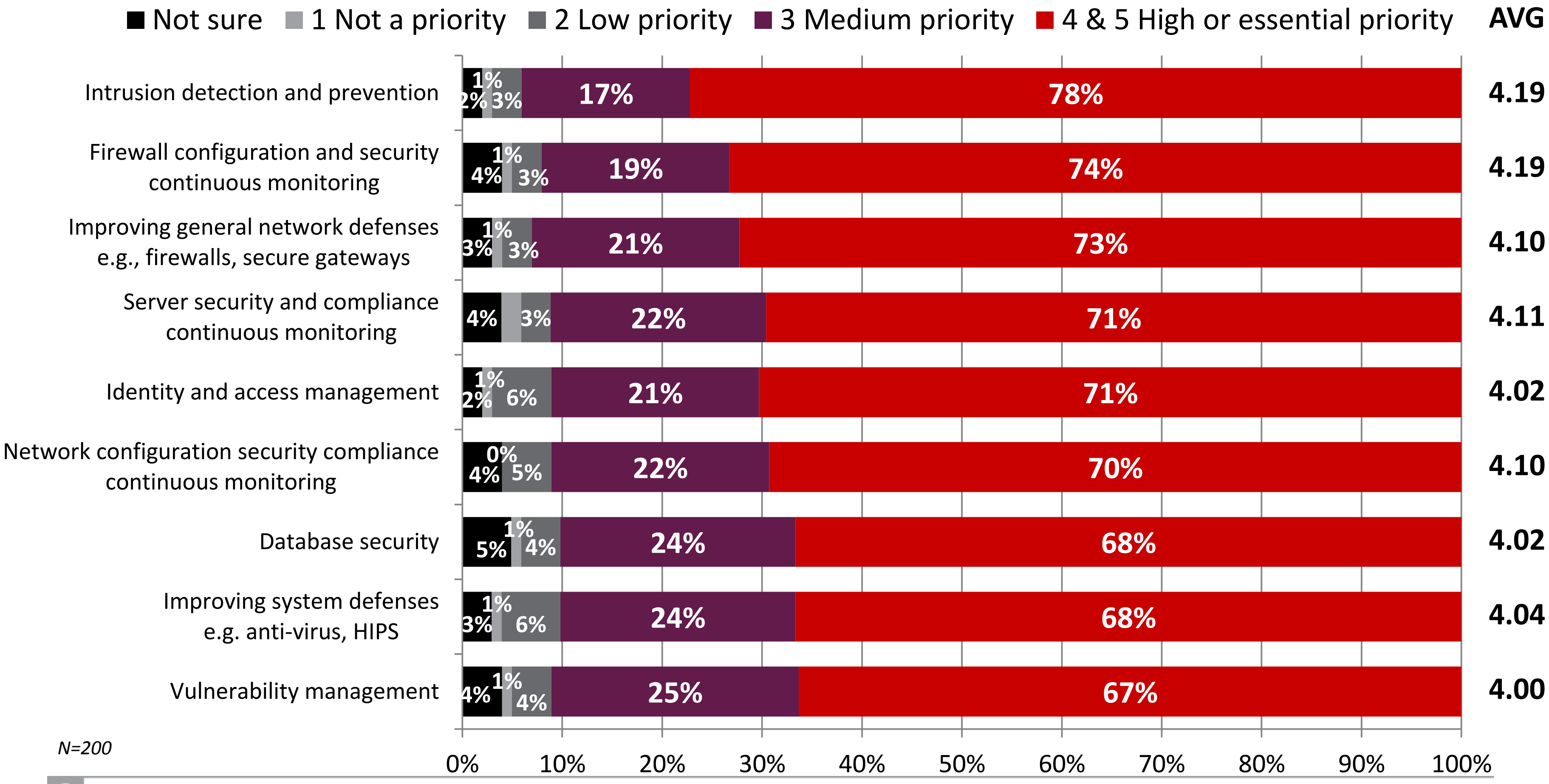
Note: Multiple responses allowed

○ = statistically significant difference

Q *What are the largest sources of security threats to your agency? (select all that apply)*

Security Investment Priorities

- Firewall configuration and security continuous monitoring are the top essential priorities for investing resources in the next 12 months.

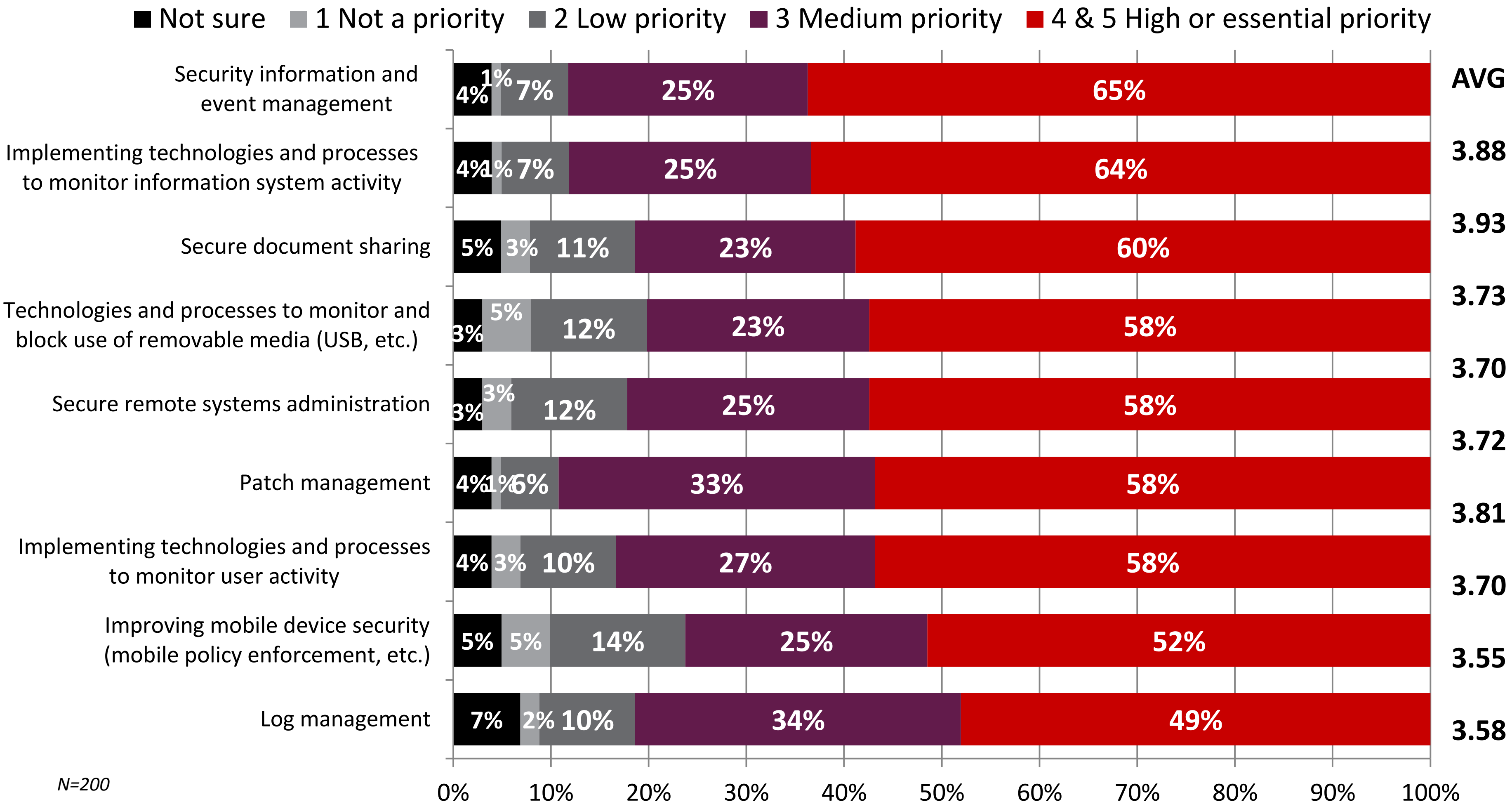


N=200

Q *For each of the following security practices and/or technologies, please indicate your organization's priority level for investing resources in the next 12 months.*

Security Investment Priorities (Continued)

solarwinds



N=200

Q *For each of the following security practices and/or technologies, please indicate your organization's priority level for investing resources in the next 12 months.*

Security Investment Priorities (Continued)

solarwinds

- Continuous monitoring users indicate that most practices and technologies are of essential priority investments significantly more than non-users.

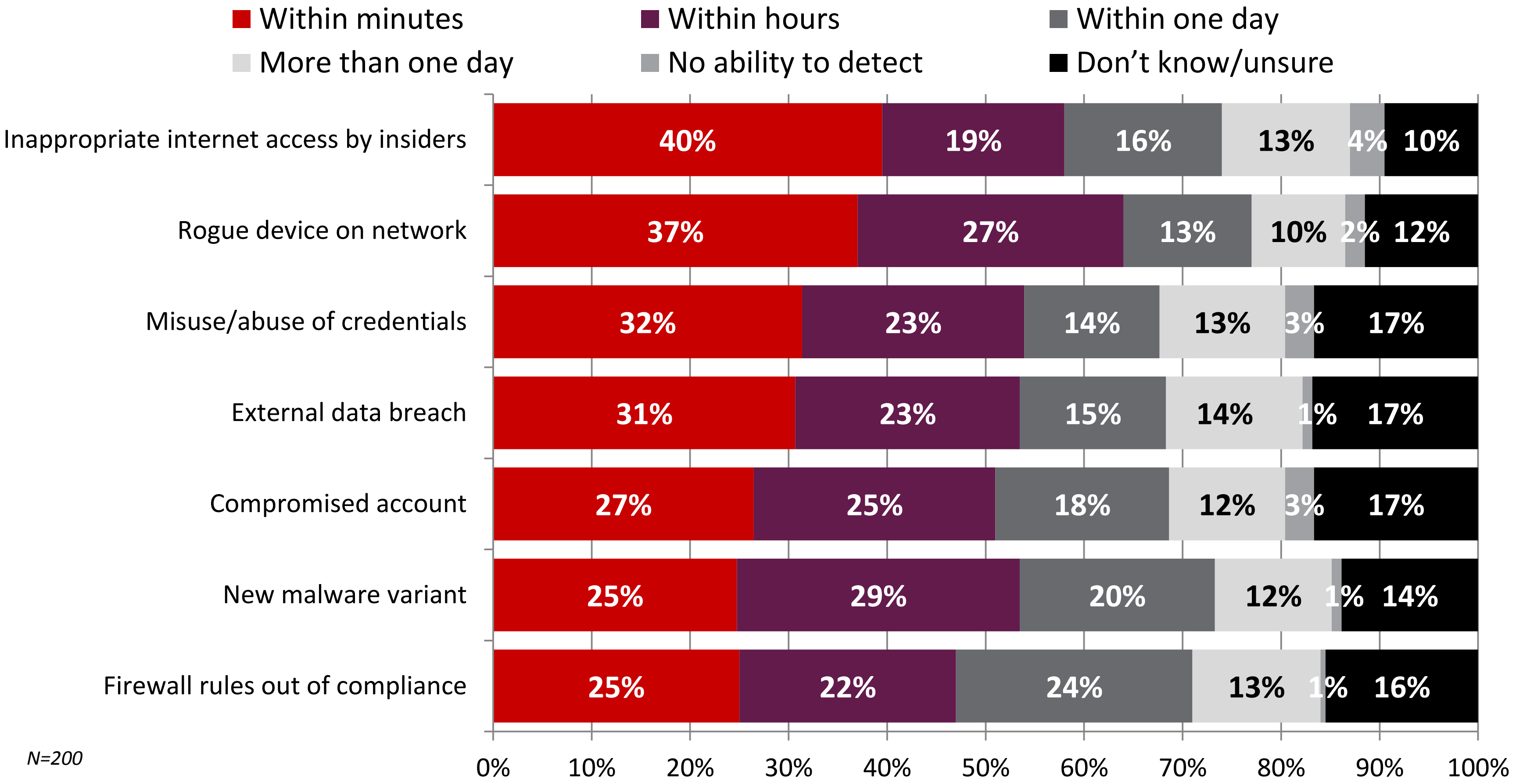
5 - Essential		
	Continuous Monitoring User	Non-User
Firewall configuration and security continuous monitoring	53%	33%
Intrusion detection and prevention	52%	31%
Improving system defenses e.g. anti-virus, HIPS	46%	32%
Network configuration security compliance continuous monitoring	46%	31%
Database security	44%	17%
Vulnerability management	41%	25%
Technologies and processes to monitor and block use of removable media (USB, etc.)	37%	23%
Secure remote systems administration	36%	20%
Security information and event management	34%	20%
Patch management	33%	19%

○ = statistically significant difference

Q *For each of the following security practices and/or technologies, please indicate your organization's priority level for investing resources in the next 12 months.*

Security Event Detection

- Respondents report most often that inappropriate internet access by insiders can be detected within minutes.

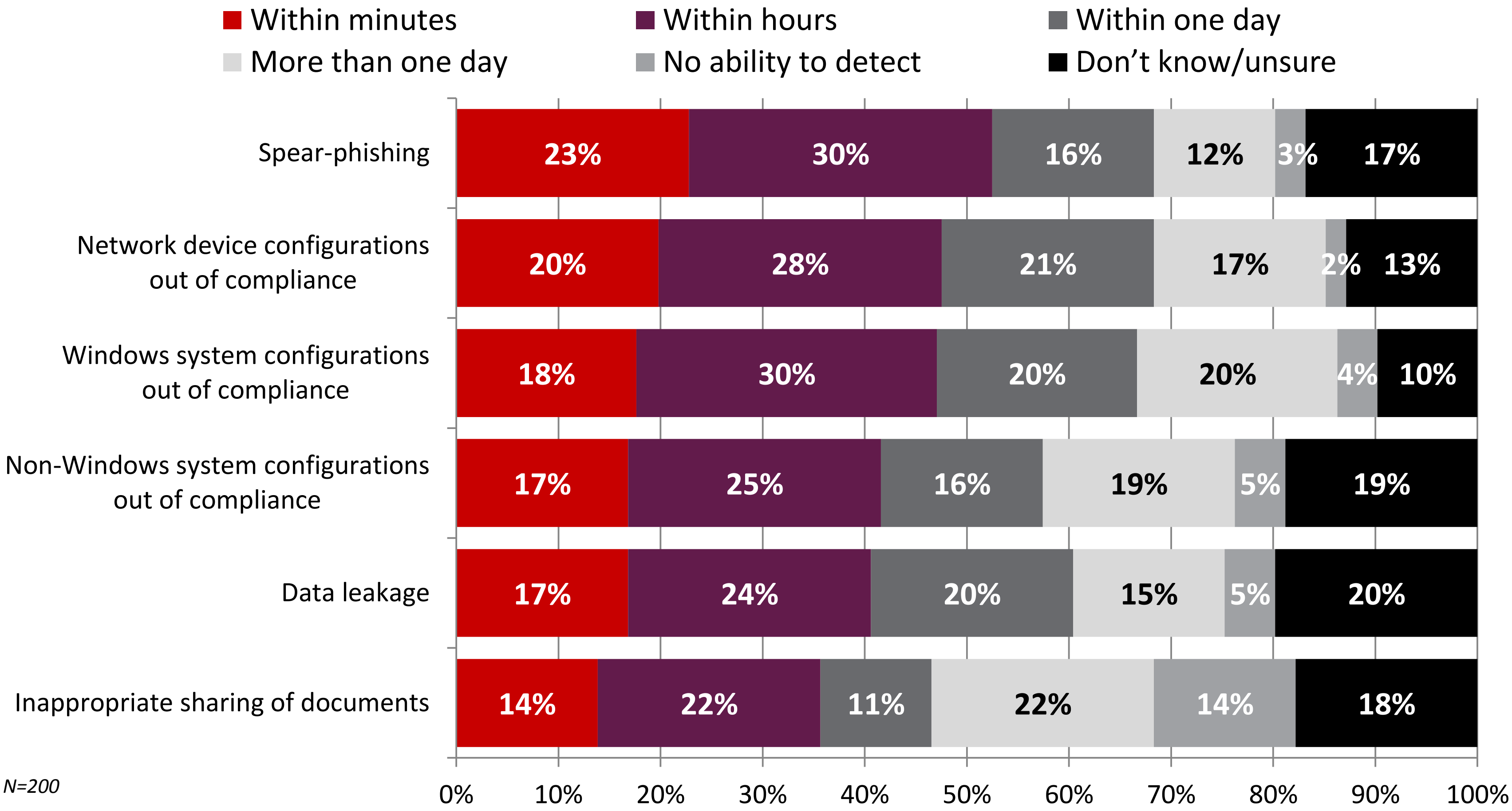


N=200

Q *How long does it typically take your organization to detect and/or analyze to the following types of security events or compliance issues?*

Security Event Detection (Continued)

- Inappropriate sharing of documents is reported least as being able to be detected within minutes.



Q *How long does it typically take your organization to detect and/or analyze to the following types of security events or compliance issues?*

Security Event Detection (Continued)

solarwinds

- Continuous monitoring users indicate detecting and analyzing most security events or compliance issues within minutes significantly more than non-users.

Within Minutes

	Continuous Monitoring User	Non-User
Inappropriate internet access by insiders	46%	29%
Rogue device on network	46%	23%
Misuse/abuse of credentials	37%	23%
Compromised account	34%	15%
Firewall rules out of compliance	30%	16%
Windows system configurations out of compliance	23%	8%
Data leakage	22%	8%

○ = statistically significant difference

Q *How long does it typically take your organization to detect and/or analyze to the following types of security events or compliance issues?*

Contact Information

Market Connections
Research you can act on.

solarwinds

Laurie Morrow, Director of Research Services | Market Connections, Inc.

14555 Avion Parkway, Suite 125 | Chantilly, VA 20151 | 703.378.2025, ext. 101
LaurieM@marketconnectionsinc.com

Lisa M. Sherwin Wulf, Federal Marketing Leader | SolarWinds

703.234.5386
Lisa.SherwinWulf@solarwinds.com
www.solarwinds.com/federal
@SolarWinds_Gov