Solarwinds Public Sector **Cybersecurity Report 2021**

Market Connections® Research you can act on.

solarwinds government

Change in an Evolving Cyber Landscape

Organizations Host IT Security Products Across **Multiple Locations**

Half Prefer Cloud Locations

81% On-premises
68% Government Private Cloud
56% Hybrid Cloud
52% Public Cloud
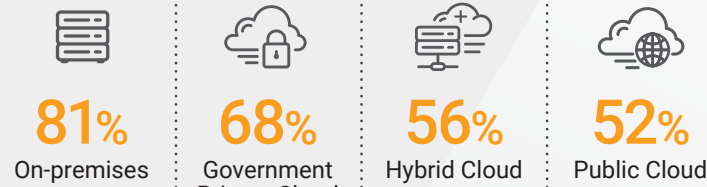
8 out of 10 currently host products **on-premises**

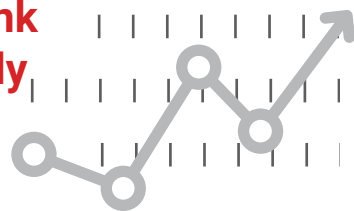**Over 1/2** prefer to host products on some form of **cloud** (private/public/hybrid)

The Impact of **Zero-Trust Strategy**

2/3 of respondents **do not** have a formal zero-trust strategy in place

AND 1 in 5 are **not currently using** or **considering** a zero-trust approach

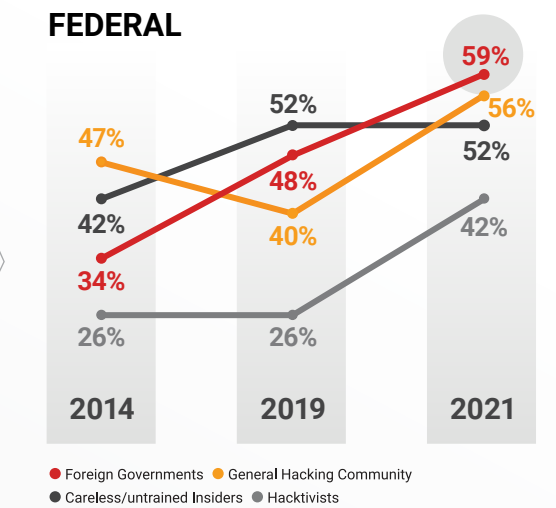## **Prioritizing** Executive Order Objectives

Respondents Rank All Almost Equally

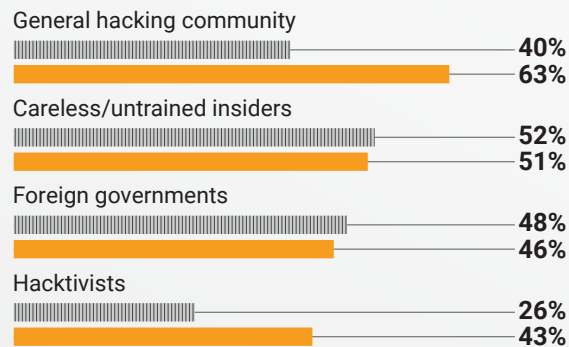| OBJECTIVE	AVG. RANK
Improve investigative and remediation capabilities	3.89
Improve barriers to sharing threat information	3.91
Create a standard playbook for cyber incident response	3.95
Improve detection of incidents on networks	4.01
Improve software supply chain security	4.03
Establish cybersecurity safety review board	4.04
Modernize and implement stronger standards	4.18

Top Concerns Over Source of Security Threats Grow and Show Major Changes

Among Federal Agencies, Foreign Governments Rise to Top while Careless Insiders are Bumped to Third
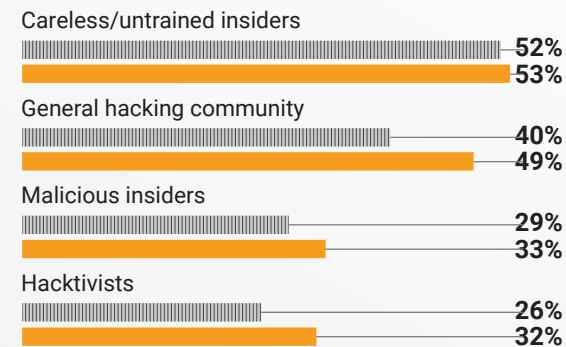
FEDERAL

	2014	2019	2021
Foreign Governments	34%	48%	59%
General Hacking Community	47%	40%	56%
Careless/untrained Insiders	42%	52%	52%
Hacktivists	26%	26%	42%

Legend: ● Foreign Governments ● General Hacking Community ● Careless/untrained Insiders ● Hacktivists

For SLED, General Hacking Community and Careless/Untrained Insiders are Top Concern

■ 2019 ■ 2021

STATE & LOCAL

	2019	2021
General hacking community	40%	63%
Careless/untrained insiders	52%	51%
Foreign governments	48%	46%
Hacktivists	26%	43%

EDUCATION

	2019	2021
Careless/untrained insiders	52%	53%
General hacking community	40%	49%
Malicious insiders	29%	33%
Hacktivists	26%	32%

Top Impediments to Detection and Remediation of Security Issues

Training and Resources Tops List

- **40%** Insufficient training of IT staff to detect/respond/remediate
- **37%** Shortage of funding and resources
- **32%** Expanded security perimeter due to worker volume
- **31%** Insufficient collection/monitoring of data to correlate/detect
- **30%** Insufficient user awareness training
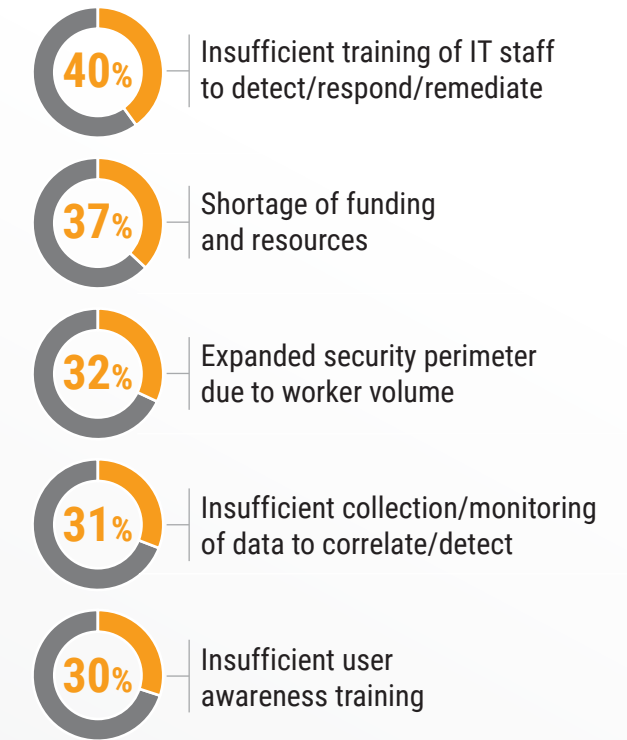
Are Constantly Changing Requirements Creating a **Prioritization Bottleneck?**

IT SECURITY		INFRASTRUCTURE		MODERNIZATION	
Intrusion detection and prevention	68%	Remote access capabilities	62%	Replace legacy applications	60%
Access management	67%	Collaboration tools	61%	Migrate systems to cloud	60%
Vulnerability management	65%	Improve troubleshooting	59%	Virtualize/consolidate data center	59%
Security event and incident management	65%	Remote support tools	59%	Utilize digital services	59%
Improve compliance	65%	Network core	58%		
Education and training	63%	Capacity planning and optimization	58%		
Implementing zero-trust framework	61%	Disaster preparedness	58%		