MeriTalk
Improving the Outcomes of Government IT

splunk>
turn data into doing™

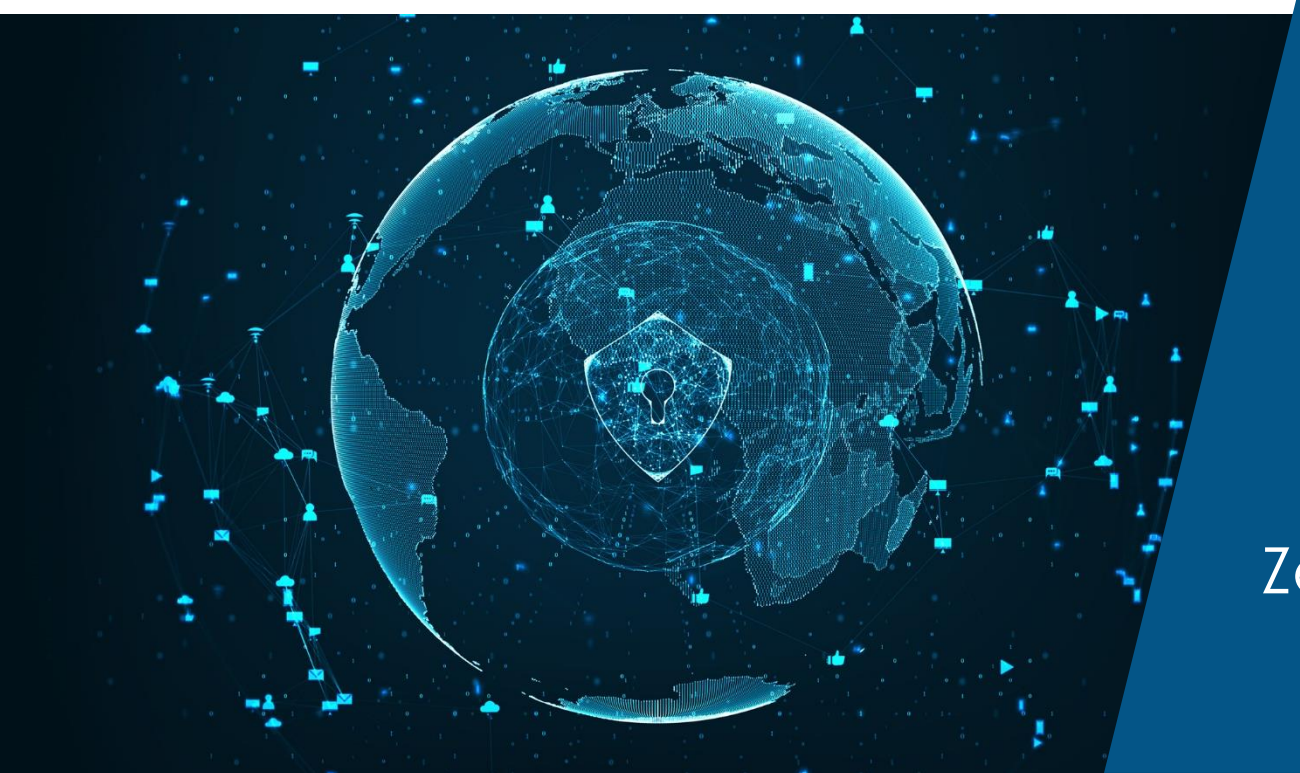
augustschell

BLACKWOOD

ClearShark
fierce technology solutions

Red River

World Wide Technology



PUBLIC SECTOR SECURITY IN A MODERN WORLD: Implementing a Zero Trust Mentality

Introduction

A catalyst for change, the transition to "maximized telework" forced public sector organizations to rapidly modernize their approach to IT. But how is the need for modernization affecting cyber strategies, like the adoption of **zero trust**?

What's driving organizations to consider a zero trust framework, and what challenges are they facing?

MeriTalk surveyed **150 Federal and 150 state, local and higher education (SLED) IT decision makers** to explore zero trust progress and future priorities, and reveal opportunities to increase confidence and trust in public sector security.

Executive Summary

MeriTalk
Improving the Outcomes of Government IT

Public sector organizations are turning to zero trust to fortify their cybersecurity posture:

86% of public sector IT decision makers say a zero trust approach will help make their organization more resilient

81% say their organization has made changes to its cybersecurity strategy to formally include and/or define a zero trust approach

Still, some doubt their ability to execute on a zero trust framework:

Just **55%** are very confident in their organization's ability to execute on a zero trust framework

78% face mission challenges and **75%** face technical challenges implementing a zero trust approach

To turn interest into action, IT leaders must invest in both technical and cultural change:

While **83%** see value in a data-driven analytics approach to security, just a little over a third have implemented key foundational solutions like SIEM, SOAR, UEBA, and CDM

To advance, IT leaders recommend permeating the culture with a zero trust philosophy, establishing senior leadership buy-in, and prioritizing funding

Mounting Complexity

- Growing complexity, costs, and cloud environments encourage public sector security leaders to rethink their cyber strategies with greater urgency

With digital transformation initiatives and the shift to remote work, which of the following has your organization experienced?*

#1 Increased complexity

#2 Increased cost

#3 Increased use of hybrid and/or multi-cloud environments

#4 Increased risk to organizational assets and resources

#4 Increased security incidents

#4 Increased use of automation and AI/ML in security initiatives

#7 Increased use of unapproved devices

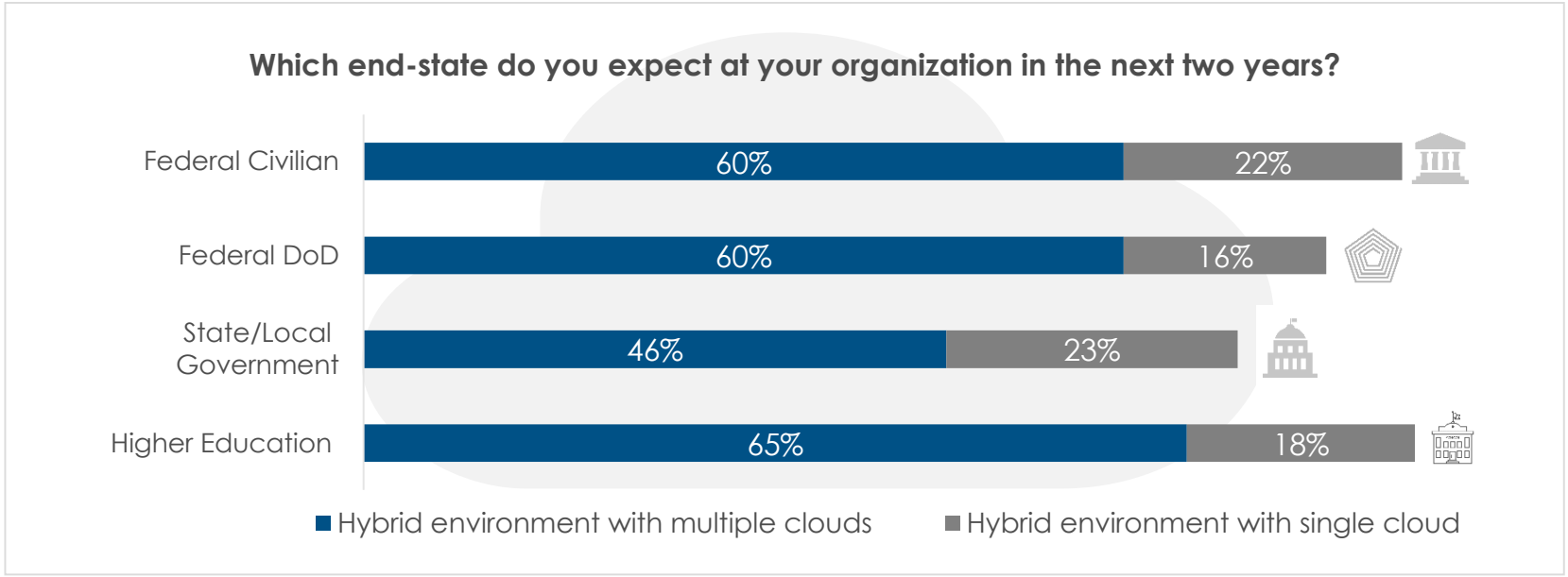
#8 Increased shadow IT

Takeaway: Urgent Need for Greater Visibility and Security Management

*Respondents asked to select all that apply

Critical for Cloud

- **85%** of public sector IT decision makers agree a zero trust approach is essential to managing risk in a hybrid and/or multi-cloud environment



Takeaway: Zero Trust Approach Is Critical for Cloud Futures

A New Approach

- The vast majority of public sector IT decision makers are turning to zero trust to fortify their security posture in this changing landscape

81% say their organization has made changes to its cybersecurity strategy to **formally include and/or define a zero trust approach**

54% of that group did so since the shift to remote work

86% say a zero trust approach is essential to securing a modern, **remote workforce**

86% say a zero trust approach will help make their organization **more resilient**

Takeaway: Adopt or Fall Behind

Zero Trust Drivers

MeriTalk
Improving the Outcomes of Government IT

What are the primary drivers for your organization to consider a zero trust framework?

Federal Civilian Agencies

- **Mission driver**: Increased shift to remote work (54%)
- **Technical driver**: Improved anomalous behavior detection and response (45%)

State/Local Government

- **Mission driver**: Increased shift to remote work (44%)
- **Technical driver**: Improved control over unmanaged and/or unapproved device access (41%)

Federal DoD Agencies

- **Mission driver**: Improved ability to deliver on mission objectives securely (38%)
- **Technical driver**: Improved High Value Asset (HVA) security (36%)

Higher Education

- **Mission driver**: Increased shift to remote work (44%)
- **Technical driver**: Improved compliance (38%)

Takeaway: Telework & Security Management Needs Spur Change

What's Holding Organizations Back?

- Despite progress, public sector IT decision makers lack confidence in their ability to execute on a zero trust framework

While **80%** are actively adopting zero trust principles,

Just **55%** are very confident in their organization's ability to execute on a zero trust framework

Takeaway: Agencies Lack Confidence in Their Ability to Execute

Adoption Challenges

- When it comes to implementing zero trust, **three out of four** of public sector organizations say they're facing mission and/or technical challenges

78% face
mission challenges

75% face
technical challenges

Top mission challenges?*

#1 Lack of skilled professionals

#2 Lack of funding

#3 Organizational silos

#3 Lack of strategy to adopt

Takeaway: Lack of Resources and Buy-in Stalls Progress

*Respondents asked to select all that apply

Adoption Challenges (Cont.)

MeriTalk
Improving the Outcomes of Government IT

Top technical challenges?*

Federal Civilian Agencies

- **#1**: Lack of automation capabilities to drive fast risk mitigation
- **#2**: Increased amounts of shadow IT

State/Local Government

- **#1**: Too many disparate products to drive a single view across the enterprise
- **#2**: Increased amounts of shadow IT

Federal DoD Agencies

- **#1**: Lack of robust partner access capabilities and/or ability to manage supply chain risk
- **#2**: Lack of robust privilege management capabilities

Higher Education

- **#1**: Lack of continuous monitoring and diagnostics capabilities
- **#2**: Lack of robust privilege management capabilities

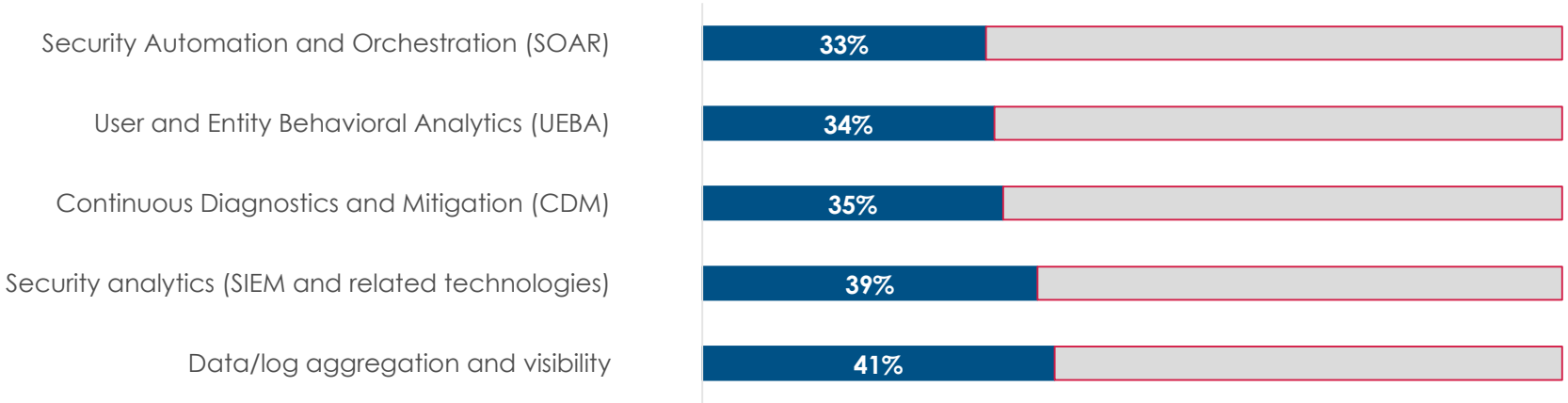
Takeaway: Investments in Visibility and Automation Are Key

*Respondents asked to select all that apply

Initial Progress

- While **83%** say a data-driven analytics approach to security will improve their ability to manage organizational risk, **60% or more** have yet to invest in key zero trust technologies

Which zero trust components do organizations have in place today?*



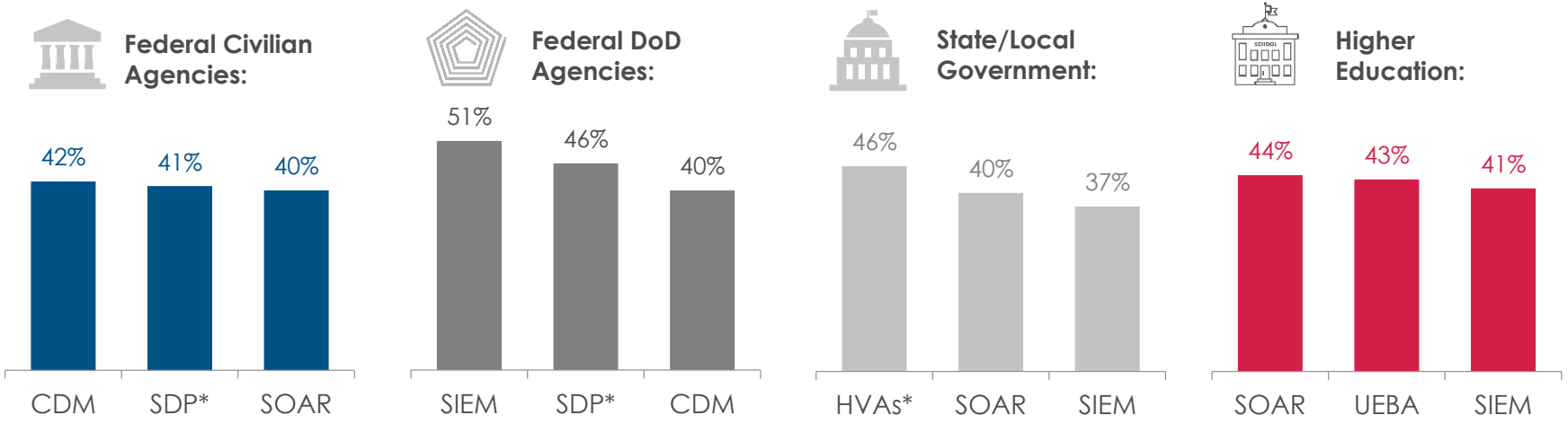
Takeaway: Propel Forward with Foundational Tech

*Respondents asked to select all that apply

What's Next?

- Over the next two years, **78%** of public sector IT leaders say their organization will increase spending on zero trust

Where are organizations focusing short-term investments?



Takeaway: Priorities Vary by Sector

*Micro-segmentation/Software-Defined Perimeter (SDP); Complete asset inventory including High Value Assets (HVAs)

Who's Doing It Right?

- **35%** of public sector IT leaders describe their organization's zero trust adoption as 'advanced,' saying they are **aggressively adopting zero trust principles**

Advanced organizations are significantly more likely to:

Plan ahead:	**44%** formally defined zero trust in their cybersecurity strategy ahead of the shift to remote work vs. just **18%** of novice organizations
Focus on the mission:	**44%** say increasing their ability to deliver on mission objectives securely is driving zero trust adoption vs. **21%** of novice organizations
Double down:	**50%** say they will significantly increase 2021 investments in zero trust vs. just **21%** of novice organizations

Advanced zero trust organizations are also significantly more likely than novice organizations to feel '**very confident**' in their current security capabilities:

79%  to **46%** 

Takeaway: Learn from the Leaders

Necessary Resources

- Looking ahead, public sector organizations need training and security analytics capabilities to successfully implement a zero trust architecture

Aside from funding, what does your organization need to successfully implement a zero trust architecture?*

#1 Awareness and training on zero trust principles

#2 Security and behavior analytics capabilities

#3 Data management and visibility

#3 Security automation capabilities

#3 Ability to calculate risk posture of connecting entities in real-time

86% say their security approach should **assume their network is already penetrated** or will be in the near future

Takeaway: Awareness and Advanced Analytics Are Required

*Respondents asked to select all that apply

Guidance for the Future

- IT leaders suggest permeating the culture with a zero trust philosophy, acquiring senior leadership buy-in, and prioritizing funding

What advice you would give to other public sector decision makers looking to implement zero trust within their organizations?

"Zero trust should be implemented with **senior leadership buy-in** at the start; it'll make the process much easier"

"Zero trust will work best if the agency's **culture is permeated with the philosophy**"

"**Prioritize funding** for zero trust before it's too late"

"Make security the main priority and ensure that **employees are well-trained** and educated about zero trust"

Takeaway: Embrace a Zero Trust Mindset

Recommendations

Cultivate a Zero Trust Culture: To successfully implement a zero trust framework, public sector organizations must view zero trust as a mindset, rather than as a set of tools. Increase training and awareness for all staff to permeate a zero trust philosophy throughout the organization.

Mind the Gap: Despite progress, public sector IT decision makers lack confidence in their ability to execute on a zero trust framework. Overcome the confidence gap by investing in visibility and control throughout all environments and bringing in experienced partners to help coordinate efforts.

Focus on Foundational Tech: Only a third of Federal and SLED IT managers say their organization has key zero trust components in place. Advance zero trust efforts by implementing data-driven solutions like security automation, security and behavioral analytics, and continuous monitoring.

Methodology & Demographics

MeriTalk, on behalf of Splunk, conducted an online survey of 150 Federal and 150 state, local, and higher education (SLED) IT decision makers familiar with their agency's cybersecurity efforts in October 2020. At a 95% confidence interval, the standard margin of error is ±5.62%.

Respondent job titles

CIO/CTO/CISO	14%
Deputy CIO/CTO/CISO	7%
IT Director/Vice President	36%
Cybersecurity Manager/Supervisor	14%
Data Center Manager/Supervisor	6%
Information Assurance Manager/Supervisor	11%
Program/Project Manager	9%
Cybersecurity Acquisitions/Procurement Manager	3%

Organization types

Federal Government: Civilian Agency	26%
Federal Government: DoD or Intelligence Agency	24%
State Government	18%
Local Government	11%
Higher Education	21%

Expertise

100% of qualifying respondents help design, implement, or enforce decisions regarding their organization's current cybersecurity capabilities and/or future strategies

Thank You

www.meritalk.com

research@meritalk.com

703-883-9000 ext. 128