Market Connections™
Research you can act on.
A portfolio platform of GovExec

Navigating Challenge, Seizing Opportunity

The State of Zero Trust in Federal and State and Local Government

February 2024

Sponsored by:

LUMEN®

Introduction

Complete Zero Trust adoption is a journey — one with a constantly evolving landscape. For example, in 2021 when the first version of the CISA (Cybersecurity and Infrastructure Security Agency) Zero Trust Maturity Model came out, AI was just beginning to enter in the discussions. That has changed. Not only is AI now a focus of virtually all federal IT discussions, some agencies are already looking toward Quantum computing. These days, Zero Trust can feel like yesterday's news.

But it most definitely is not. It is, perhaps, more critical than ever. So much so that CISA released the "Zero Trust Maturity Model Version 2" in April, 2023. Other versions will no doubt follow.

Six months after that updated release of the CISA guidance, Lumen partnered with market research firm Market Connections to assess where federal agencies stand regarding zero trust adoption, and to determine to what extent they have been utilizing Managed Security Operations Centers (SOCs) to enhance their security posture, and the next steps for the Zero Trust adoption journey.

Knowledge and Strategy: Building the Foundation

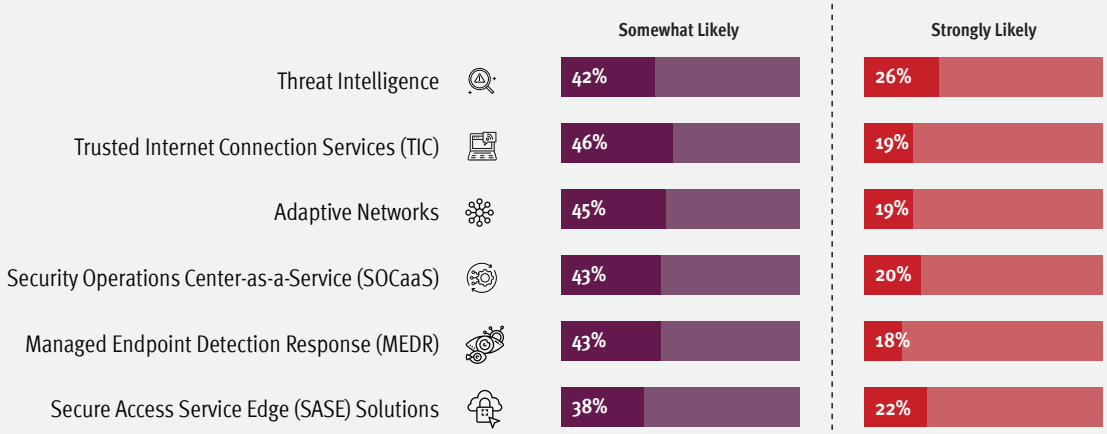
The study reveals a dichotomy between respondents' knowledge of Zero Trust concepts and their agencies' strategic considerations. Familiarity with threat intelligence is high, with 78% of respondents knowing at least at little about it. The majority are also familiar with Security Operations Centers as a Service (SOCaaS) (71%). Secure Access Service Edge (SASE) solutions and Managed Endpoint Detection and Response (MEDR) lag behind. This knowledge gap mirrors agencies' strategic priorities, with threat intelligence topping the list of considered strategies. SOCaaS are part of the strategy, though—60% of are considering it. That puts SOCaaS on par with SASE for strategic consideration.

KNOWLEDGE LEVELS

	I Know A Little	I Know Quite A Bit	I'm An Expert
Threat Intelligence	42%	34%	4%
Trusted Internet Connection Services (TIC)	43%	22%	6%
Adaptive Networks	46%	20%	5%
Security Operations Center-as-a-Service (SOCaaS)	40%	24%	6%
Managed Endpoint Detection Response (MEDR)	33%	22%	6%
Secure Access Service Edge (SASE) Solutions	36%	20%	5%

Q: How would you classify your knowledge of each of the following?

STRATEGY CONSIDERATION

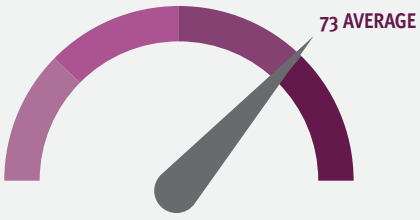


Q: How likely would you be to consider any of the following offerings as part of your Zero Trust strategy?

Confidence and Concerns: Embracing Change Amidst Challenges

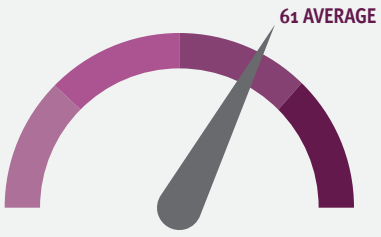
Despite some knowledge gaps, respondents express an overall confidence in their agencies' existing cybersecurity strategies. Nearly all respondents rate their agency's approach 50 or higher on a 0–100 scale, indicating a solid foundation. This confidence is likely tied to the fact that they feel their agency is well on the way to adopting and implementing a Zero Trust approach to security. Yet, there are myriad challenges agencies must address.

CONFIDENCE IN AGENCY'S CURRENT CYBERSECURITY STRATEGY



Federal	State/Local
73	73

ADOPTING AND IMPLEMENTING ZERO TRUST



Federal	State/Local
63	59

Q: How confident are you in your agency's cybersecurity strategy? On a scale of 1 to 100 where 0 is "not even on the radar yet" and 100 is "fully implemented," how far along is your organization in terms of adopting and implementing a Zero rust approach to security?

Challenges to Implementation

Lack of internal cyber security expertise is the largest workforce challenge for nearly three quarters of respondents. Finding cybersecurity professionals with the requisite skillset and expertise follows close behind, prompting a need for targeted talent development programs and upskilling initiatives. Additionally, continuously improving threat detection capabilities and integrating Zero Trust with legacy infrastructure pose significant technical challenges that require innovative solutions.

Implementing a Zero Trust approach hinges not just on technology and resources, but also having leadership that champions the Zero Trust vision. Respondents find a lack of leadership embracing change to be the biggest management challenge. Changing the culture around cybersecurity is also top of mind. These findings highlight the need for clear communication, strong leadership engagement, and fostering a culture of security awareness across all levels of the organization.

WORKFORCE CHALLENGES

	Very Important	Absolutely Essential
Finding cyber professionals	54%	18%
Finding professionals with the right level of skill	48%	24%
Lack of internal IT staff expertise	52%	18%
Training/re-skilling of employees	42%	28%
Retaining employees	43%	23%
[S&L] Finding professionals within my state/city	48%	19%
Lack of internal resources to manage	50%	15%
Lack of internal resources to implement	48%	16%
Resistance to change among users/employees	46%	15%

Q: When it comes to the workforce, how important is each of the following when considering/trying to implement a Zero Trust approach to security?

TECHNOLOGY CHALLENGES

	Very Important	Absolutely Essential
Continually improving threat detection	46%	37%
Continuous monitoring	38%	37%
Integration	48%	26%
Appropriate tools	51%	23%
Rebuilding /replacing existing legacy infrastructures	41%	29%
Automation	47%	20%
Filtering and analytics metrics	43%	21%
Visibility to entire stack	47%	14%

Q: When it comes to technology, how important are each of the following when considering/trying to implement a Zero Trust approach to security?

MANAGEMENT CHALLENGES

Leadership/upper management embracing change

Very Important	Absolutely Essential
45%	35%

Changing my organization's culture around cybersecurity

Very Important	Absolutely Essential
57%	19%

Making zero trust an organizational priority

Very Important	Absolutely Essential
48%	26%

Management having the appropriate cyber knowledge/background

Very Important	Absolutely Essential
50%	23%

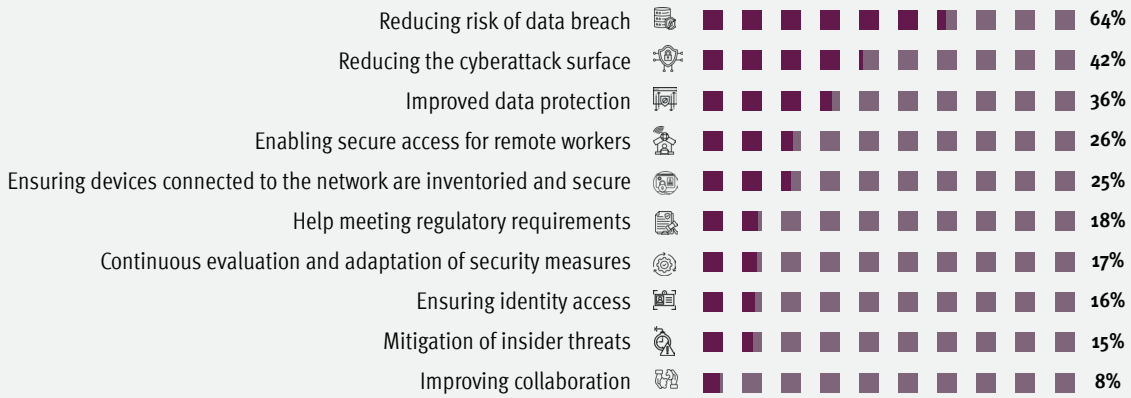
Q: When it comes to management, how important are each of the following when considering/trying to implement a Zero Trust approach to security?

The Promise of Zero Trust: Benefits and Beyond

Despite the challenges, the potential rewards of embracing Zero Trust are substantial. By far the number one benefit for federal respondents is reducing the risk of data breaches. A minimized attack surface and enhanced data protection round out the top three benefits.. These advantages underscore the potential of Zero Trust to safeguard sensitive government data and bolster the nation's cybersecurity posture.

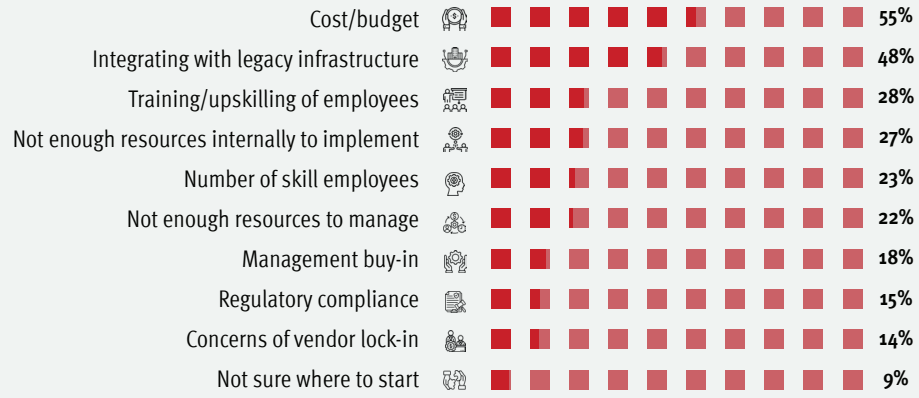
However, the road to success isn't without its roadblocks. Integrating with existing legacy infrastructure landed right behind cost as a barrier, highlighting the need for careful planning and phased implementation strategies to ensure seamless migration. Interestingly, despite the various workforce challenges cited, workforce-related issues do not seem to be barriers to implementation for the respondents.

TOP BENEFITS



Q: When thinking about implementing a Zero Trust approach to cybersecurity, what are the top benefits to your organization that you're looking for?

TOP BARRIERS



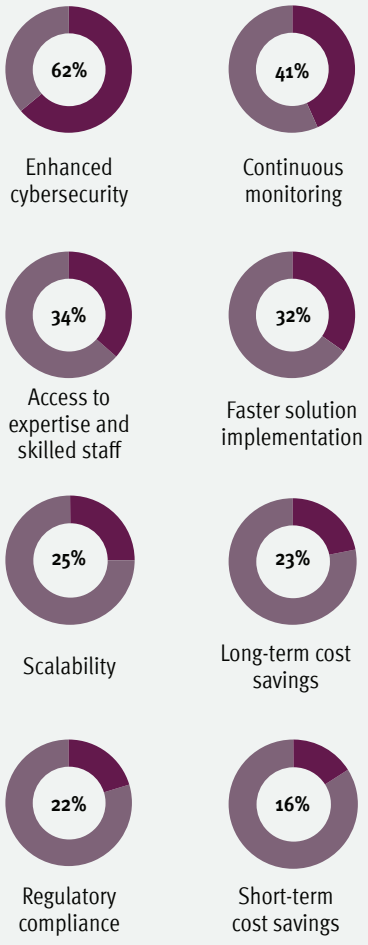
Q: When thinking about implementing a Zero Trust approach to cybersecurity, what are the top barriers for your organization?

Managed SOC Adoption

Organizations in general have been looking to enhance their security operations centers. More importantly they're looking to move to a Zero Trust Architecture, and they need to do these things while managing tight budgets. A SOCaaS offers an intriguing alternative for agencies struggling with limited resources and expertise. Respondents understand the benefits a SOCaaS can provide, including enhanced cybersecurity, continuous monitoring, and access to skilled staff. However, cost concerns and dependency on third-party providers pose significant barriers, suggesting a need for fostering trust in potential partners.

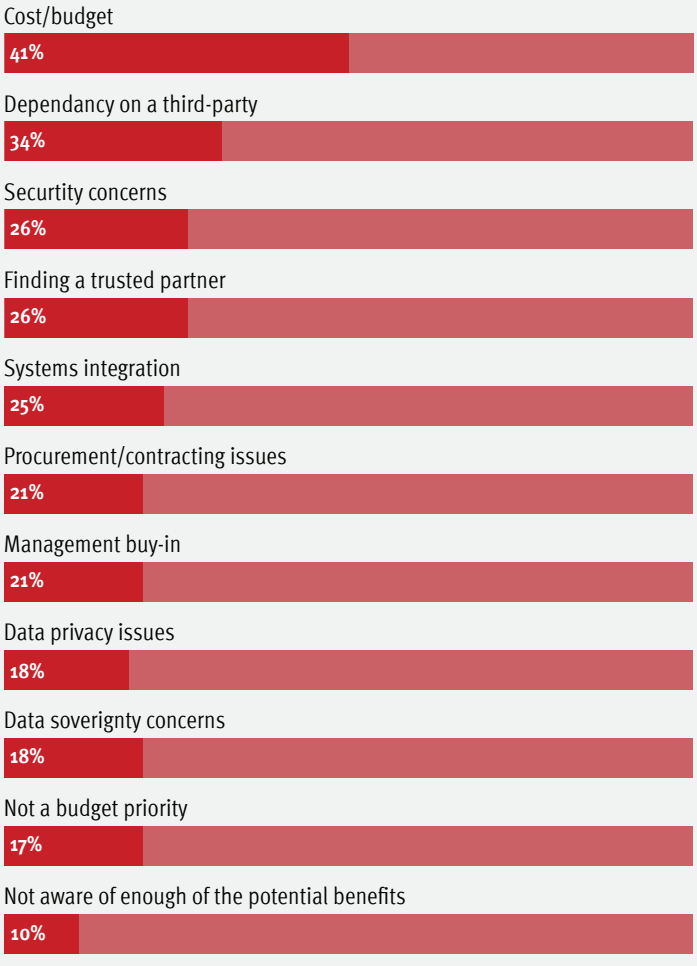
Despite these challenges, the positive perception of SOCaaS holds promise for future adoption. Nearly half of the respondents have either implemented or plan to implement SOCaaS within the next three years, highlighting its potential as a valuable tool in the Zero Trust journey.

BENEFITS OF SOCaaS

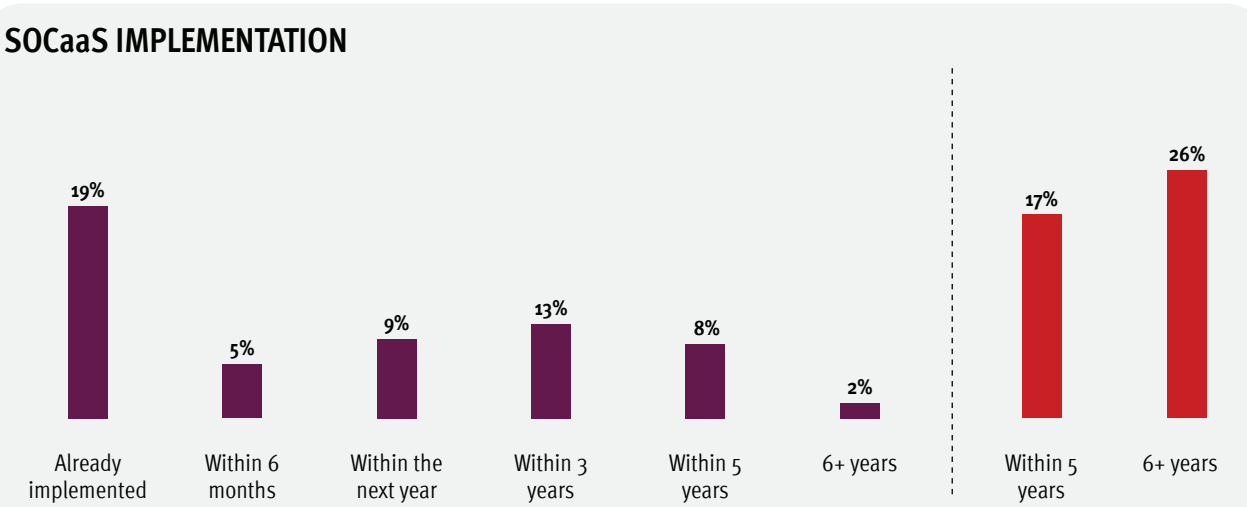


Q: What would be the biggest benefits you see to implementing Security Operations Center-as-a-Service in your organization?

BARRIERS TO SOCaaS IMPLEMENTATION



Q: What do you see as the biggest barriers to implementing Security Operations Center-as-a-Service in your organization?



Q: What is the sate of your organizations Security Operations Center-as-a-Service (SOCaaS) implementation?

What this Means for Agency Cyber Security

The current state of Zero Trust in the federal government reflects a landscape both promising and complex. Agencies acknowledge the need for transformation and are actively moving toward Zero Trust adoption. However, significant hurdles – from budgetary constraints to technological challenges – still exist. Overcoming these obstacles requires a multi-pronged approach that emphasizes leadership commitment, talent development, strategic resource allocation, and innovative solutions. Finding a partner that understands these challenges and the importance of staying focused on mission critical objectives can help agencies unlock the vast potential of Zero Trust. With a multilayered approach to user authentication, risk to critical data and infrastructure is minimized, performance is enhanced by providing employees secure and fast access to applications, and cost can be reduced through optimized infrastructure that streamlines access to environments.

Market Connections™
Research you can act on.
A portfolio platform of GovExec

ABOUT THE STUDY

Market Connections and Lumen partnered to design an online survey of 200 federal government employees and 200 state and local government employees involved in IT decision making in August – September 2023. Respondents were screened for their involvement in the selection or management of firms that provide IT security services and solutions. All respondents had some knowledge of zero trust implementation in their organization.

ABOUT LUMEN

Lumen is a global communications services provider that ignites business growth by connecting people, data and apps—quickly, securely and effortlessly. Our networking, edge cloud, collaboration, security solutions, and managed services are designed to elevate your business and deliver the most user-friendly, intuitive and productive technology environments. With agencies under pressure to meet the mandates of the Cybersecurity Executive Order, Lumen is a trusted partner that will work alongside of them on this Zero Trust journey.

For more information visit: https://www.lumen.com/public-sector.html

ABOUT MARKET CONNECTIONS

A performance platform of GovExec, Market Connections delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations, and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications; healthcare; and education.

For more information visit: www.marketconnectionsinc.com

Sponsored by:

LUMEN®