GENERAL DYNAMICS
Information Technology

ZERO TRUST RESEARCH REPORT

Agency Guide to Zero Trust Maturity

Federal IT and program managers know that implementing zero trust is a strategic approach to defend against cyber threats. Ahead of the 2024 deadline, federal agencies are making progress in their zero trust implementation. But agencies also recognize the challenges they face and know there's still important work to do.

Market Connections®
Research you can act on.

Foreword

As technology advances and our adversaries leverage more sophisticated tactics, it is incumbent upon federal agencies and their mission partners to be as prepared as possible to detect, deter, and defend against an ever-growing cyber threat. Zero trust is a multiplier to further protect their organizations.

Zero trust strategy is focused on increasing cyber resiliency and improving mission enablement. It's a cultural shift combining strategy and technology to continuously assess risk throughout the enterprise to ensure that users and operators have secure access at the right time to better execute their missions. Improving zero trust maturity increases the effectiveness of cyber resiliency rather than just compliance. The implementation of zero trust has enormous potential to amplify and accelerate cybersecurity efforts across the federal government and improve defense against cyber threats.

This report is an analysis of the progress being made by the federal government to strengthen their cybersecurity through implementation of zero trust. As agencies begin and continue their zero trust transformation, this report is designed to assist agencies with shared challenges such as establishing strategy and governance, identifying the right technologies to implement, addressing legacy infrastructure, and demonstrating the value of zero trust to agency stakeholders. In addition, this report shines a light on the significant progress that agencies have made with their cyber strategies and captures some of the benefits agencies are already seeing from zero trust.

As agencies continue to implement zero trust, it is our hope that this report helps federal agencies better inform their approach and further accelerate their efforts.

Dr. Matthew McFadden
Vice President, Cyber & Distinguished Technologist
General Dynamics Information Technology

GDIT

Market Connections®
Research you can act on.

Executive Summary

One year after the signing of the Executive Order on Improving the Nation's Cybersecurity, federal agencies are undergoing a massive transformation as they work to develop and adopt zero trust strategies that position them to meet the Office of Management and Budget zero trust requirements and establish a zero trust maturity within their organization. Zero trust is important for agencies to continually defend against ongoing cyberattacks threatening their missions.

Zero trust is not merely a collection of specific cybersecurity tools and services an agency uses. It is a different way of approaching cybersecurity. Unlike the traditional perimeter security model, which focused on trying to prevent breaches, zero trust is a resilience architecture. It assumes adversaries have already compromised the environment and focuses on continual assessment of risk, allowing or denying access to agency resources while continuing to execute the broader mission.

The 300 IT and program managers across the federal, civilian, and defense agencies surveyed for this report indicated they're making significant progress—**two-thirds of agencies say they will meet zero trust maturity requirements on time or ahead of schedule.** This progress has already achieved positive results: **92% of respondents are confident in their agency's security capabilities.** At least **half say their agency is at an optimal or advanced maturity** in all five Cybersecurity and Infrastructure Security Agency pillars. Until recently, zero trust was an obscurity for many in government, but expertise is growing and **more than a third say they are experts or are knowledgeable about zero trust.**

Agencies acknowledge that there are challenges to work through, including replacing legacy infrastructure and associated costs, identifying the right technologies, and a shortage of in-house zero trust expertise. Many of these challenges are compounded by the fact that some agencies' IT teams aren't sure what their mission counterparts need or want. One of the leading benefits of zero trust is enabling users access to the right resources at the right time, but this can be difficult to execute when IT teams and program managers are not aligned with stakeholders or don't understand what the intended outcome looks like. With approximately sixteen months left until the deadline, there remains time to address these challenges.

Federal IT and program managers recognize that implementing zero trust is a strategic approach that advances capabilities to prioritize cyber risks. What some stakeholders may not realize is that zero trust is a broad approach and not a specific technology. By developing a zero trust strategy that clearly integrates technology investments with specific mission goals, agencies are far more likely to see zero trust as an enabler of the mission that provides the right resources to the right people when they need them. Similarly, a compliance focus, though important, is causing some agencies to leave valuable investment opportunities on the table. For example, artificial intelligence (AI) capabilities vastly improve the detection and prevention of unknown threats while freeing up cyber resources to focus on strategic cyber initiatives. However, this analysis found that investment in AI technology ranked at the bottom of agency priorities.

How are federal agencies progressing on implementing zero trust? GDIT's Cyber Center of Excellence partnered with Market Connections, an independent research firm, to learn where federal agencies view their zero trust progress, the benefits and challenges they are facing, and the impact this has on the mission.

Executive Summary

1

Zero trust improves the user experience and security.
The top benefits of a zero trust approach for respondents are that the right users have the right access to the right resources at the right time (57%), followed by reducing the risk of a data breach (46%).

2

Optimal maturity is still a little way off.
Most said they are either currently at a traditional or advanced maturity level for each of the five pillars defined by the Cybersecurity and Infrastructure Security Agency; few have reached the optimal level at this time.

3

Legacy infrastructure is hard to replace.
More than half (58%) say the biggest challenge to implementing zero trust is that existing legacy infrastructures must be rebuilt or replaced. But agencies are making investments in digital transformations with 92% seeing moving to the cloud as a top priority.

4

Zero trust knowledge is growing.
Only 7% of respondents consider themselves experts in zero trust, but most have some knowledge. Agencies are working to upskill their teams as the need to adopt more robust cyber capabilities grows.

5

Collaboration between mission and IT teams is important.
50% of respondents are having trouble identifying what technologies they need. There is an opportunity to further improve alignment between IT teams and the mission owners they support.

6

Agencies are feeling confident.
More than half the respondents indicated their agency has a strategy in place, and they are actively implementing it. More than 90% are confident in their agency's ability to defend against cyber threats.

Who We Surveyed

The GDIT Cyber Center of Excellence partnered with Market Connections to implement an independent research analysis to provide insights into cybersecurity and zero trust adoption strategies highlighting ongoing challenges, issues, and concerns across the federal market.

Surveying 300 prequalified federal mission and IT decision makers, all respondents were required to be currently working for the federal government, and quotas were set for agency type. Respondents were split evenly between IT and program managers and have roles in the selection of firms that provide IT security services and solutions and the management of those firms once they have been hired or selected.

DEFENSE AGENCIES

40%

FEDERAL CIVILIAN AGENCIES

60%

Respondent Breakout by Job Title

40% IT / Management Information Systems (MIS) / Information Resources Management (IRM)

10% Engineering

15% Administration / Operations

12% Program Management

10% Professional / Technical Services

5% Executive Management / Command

5% Purchasing / Contracting

3% Finance / Budget

One year after the signing of the Executive Order on Improving the Nation's Cybersecurity, federal agencies are undergoing a massive transformation as they work to develop and adopt zero trust strategies. The survey was conducted in February 2022 following the release of the White House Office of Management and Budget's zero trust architecture strategy on January 26.

AUGUST 2020
National Institute of Standards and Technology (NIST) publishes Special Publication 800-207 outlining its zero trust architecture maturity model

FEBRUARY 2021
Department of Defense delivers its Zero Trust Reference Architecture

MAY 2021
White House issues Executive Order on Improving the Nation's Cybersecurity

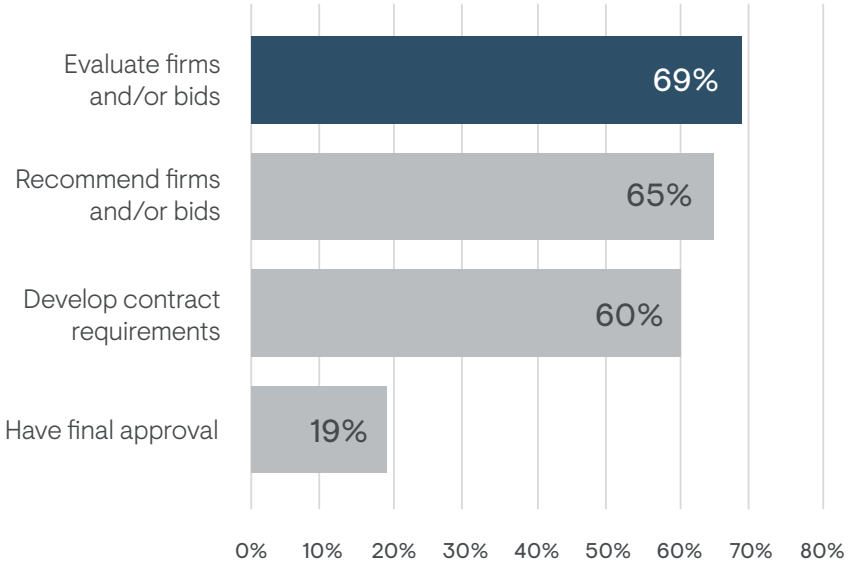
JUNE 2021
The Cybersecurity and Infrastructure Security Agency (CISA) releases a draft Zero Trust Maturity Model

JANUARY 2022
Office of Management and Budget (OMB) issues a memorandum laying out its federal zero trust architecture standards

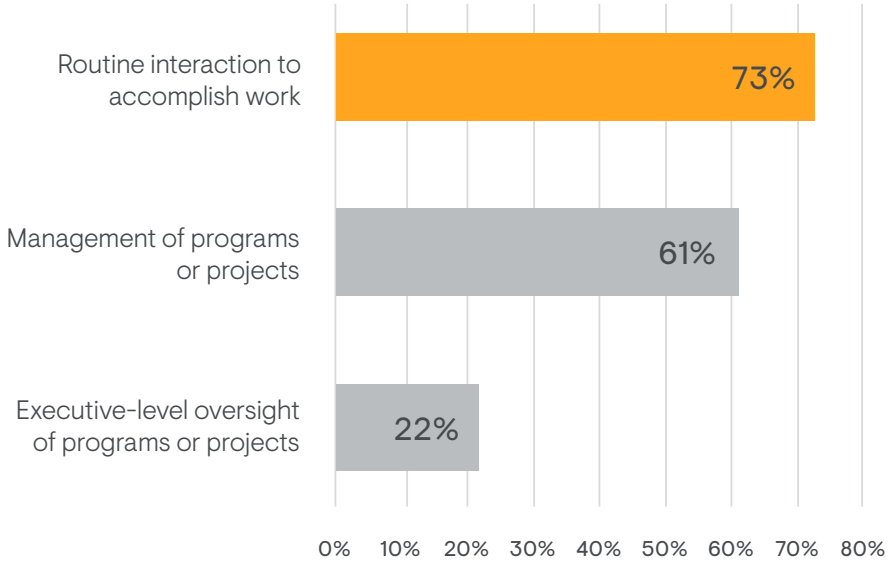
Decision Making Involvement

All respondents were screened to be involved in their organization's selection of firms that provide IT security services and solutions and the management of those firms once they have been hired or selected.

Involvement in Selection of Firms



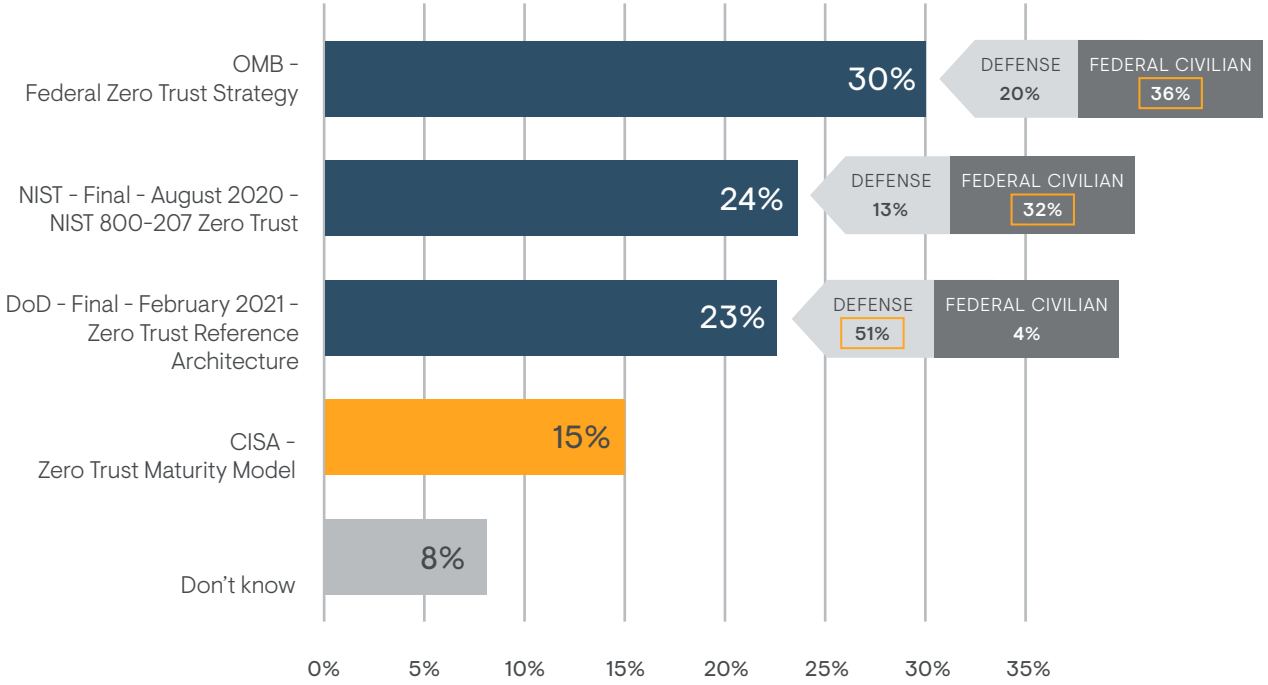
Involvement in Management of Firms Once Hired



Zero Trust Maturity In The Federal Government

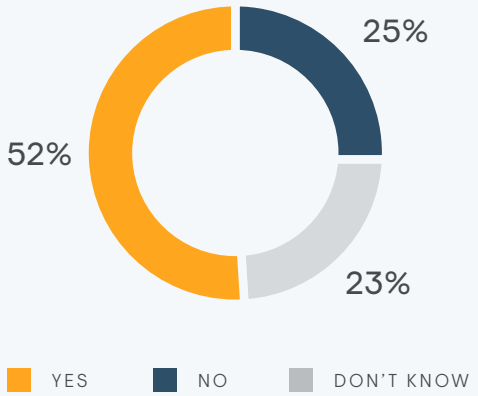
Only 15% of respondents have said they find the CISA Zero Trust Maturity Model helpful in executing their zero trust strategies even though half are following the model as a path to support the journey to zero trust. The guidance documents they do find most helpful are the OMB M-22-09 Zero Trust Strategy (30%); NIST SP 800-207 (24%); and the DOD Reference Architecture (23%). Expectedly, significantly more civilian agencies found the OMB and NIST guidance helpful and significantly more defense agencies prefer the DOD guidance.

Most Helpful Guidance for Zero Trust Implementation



statistically significant difference

Following CISA's Zero Trust Maturity Model



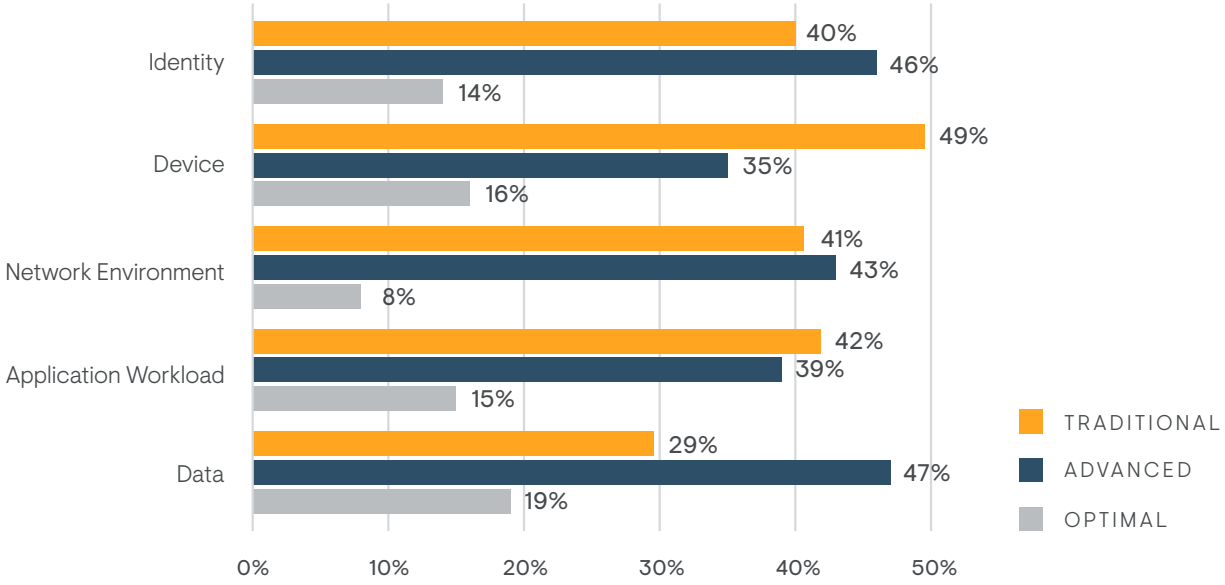
WHAT THIS MEANS

Some agencies may find different reference architectures helpful while finding CISA's maturity model best for demonstrating maturity. The CISA's maturity model provides readily understandable criteria for measuring an agency's progress as traditional, advanced, or optimal. However, other models, such as the DOD Reference Architecture, OMB Federal Zero Trust Strategy, and NIST 800-207, provide details and specifics that agencies can use for planning and budgeting specific initiatives.

Current Stage of Maturity

Using the five zero trust pillars in CISA's maturity model as a framework to assess maturity levels, the study asked respondents where they are on the journey. Most said they are either currently at a traditional or advanced maturity level; few have reached the optimal level at this time. Of all the pillars, respondents are most mature in the data pillar, though results were relatively evenly distributed.

The Five Pillars of the CISA Zero Trust Maturity Model



DATA PILLAR

For the data pillar at the traditional maturity stage, federal civilian agencies are less mature than defense agencies.

34% vs 23%

WHAT THIS MEANS

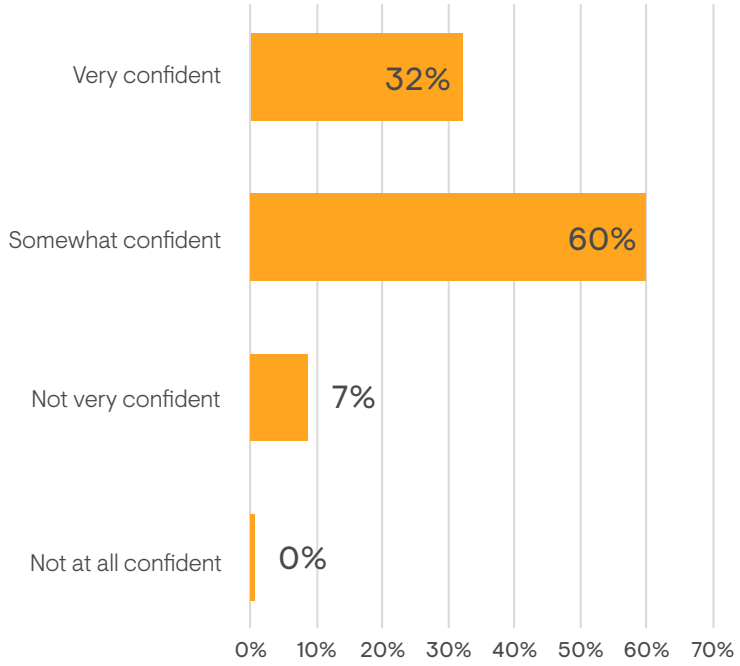
Agencies know true zero trust maturity is only achieved when you are mature across all five pillars. They are taking a steady approach in focusing on these collectively. From this data we can see that there are increasing focus areas around identity and data at the advanced level.

At an aggregate level, respondents consider their agencies most mature in the identity and data pillars. CISA lists identity as the first pillar in a successful zero trust model and zero trust is built on a foundation of identity. The maturity of identity first is largely the result of already existing requirements around federal identity and credential access management (ICAM) guidance that have already been established. Additionally, one of the key tenants of zero trust is to take a risk-based approach to allowing access to data, so it is not unexpected that agencies are also working to mature this pillar early on. Part of the increasing maturity requires more extensive enterprise-wide adoption of the capability and core technology components (e.g., enterprise Endpoint Detection and Response (EDR), micro-segmentation, zero trust network access (ZTNA) aligned across different pillars). As agencies begin to adopt and implement these new technologies holistically, we should see an increase in maturity at the advanced and optimal levels.

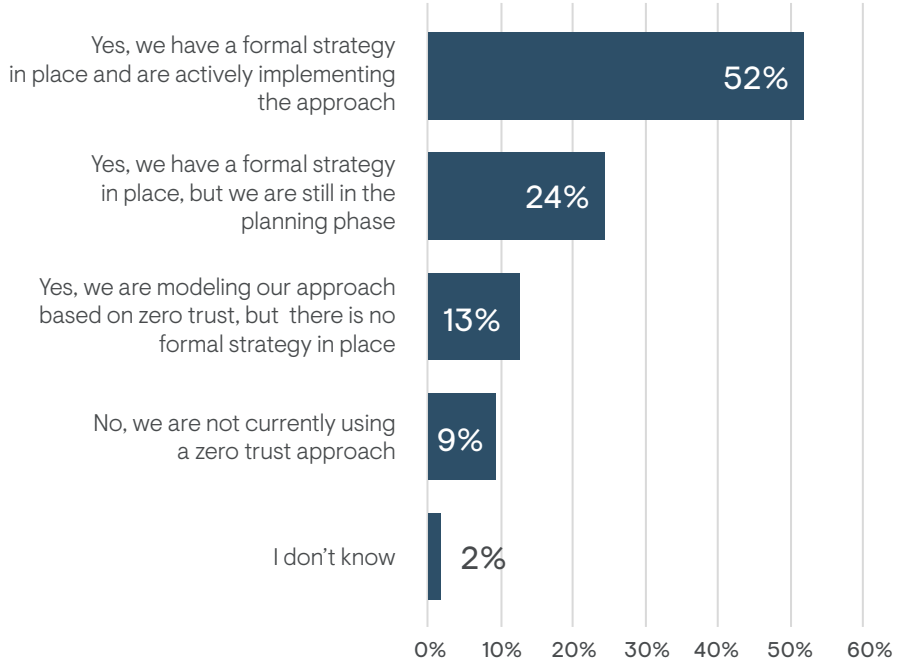
Confidence in Security and Use of Zero Trust

While just over half surveyed have a strategy in place and are actively implementing it, 92% are somewhat or very confident in their agency's security capabilities. Maturity levels do not necessarily lead to confidence in an agency's ability to defend itself from cyber threats. Agencies are still beginning to understand how zero trust must be implemented as part of their strategy to defend against ever increasing cyber threats.

Confidence in Agency's Security Capabilities



Use of a Zero Trust Approach to Cybersecurity



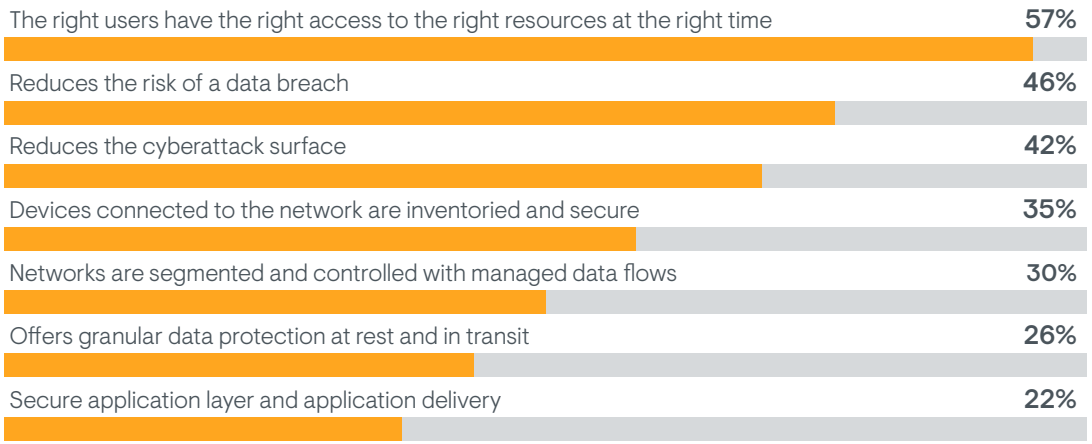
WHAT THIS MEANS

This confidence signals that many agencies have been prioritizing and addressing their greatest cyber risks and have been effective at communicating about their actions. Culture influences any effort to impart change and zero trust implementations require a targeted communications plan to prepare users for changes and help maintain awareness.

Assessing the Benefits of Zero Trust

The research identified that the top benefits of using a zero trust approach are that the right users have the right access to the right resources at the right time (57%), followed by reduced risk of a data breach (46%). Only one-quarter said offering granular data protection (i.e., encryption) at rest and in transit is a top benefit.

Top Perceived Benefits of a Zero Trust Approach to Cybersecurity

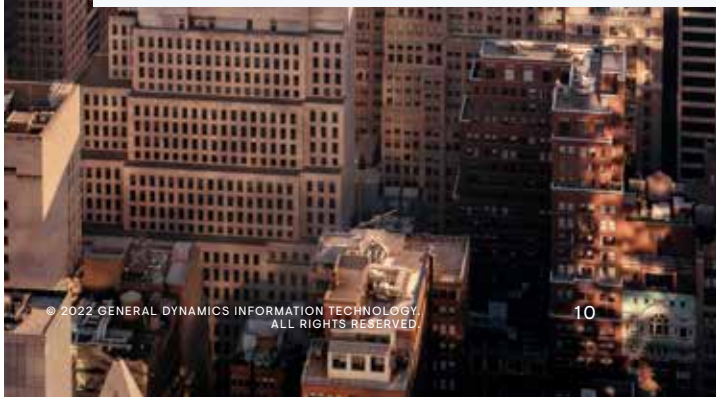


DEFENSE	CIVILIAN	BENEFIT	PROGRAM MANAGERS	IT PROFESSIONAL
63%	53%	The right users have the right access to the right resources at the right time	55%	59%
52%	42%	Reduces the risk of a data breach	51%	40%
51%	37%	Reduces the cyberattack surface	41%	44%

WHAT THIS MEANS

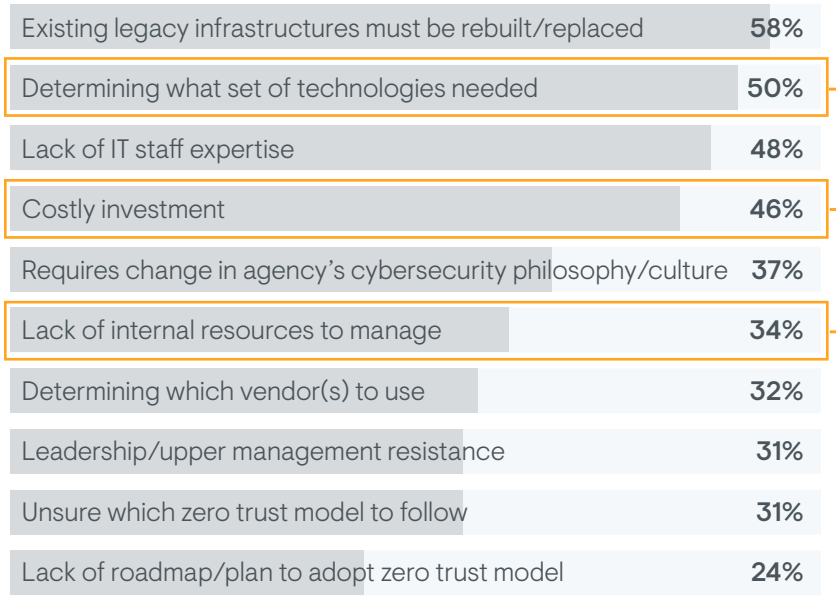
These findings are interesting because an integral component of the right users having access to the right data and application resources at the right time is enforcing granular data protection. Agencies share intelligence (i.e., data), which means they need to establish a granular data protection scheme.

Less than half (42%) of respondents said zero trust reduces the cyber-attack surface. The fact that this isn't a top benefit is notable because zero trust creates micro-perimeters that make the attack surface infinitely easier to defend and protect because it's easier to secure each individual transaction.



Challenges Implementing a Zero Trust Architecture

The biggest challenges to implementing zero trust are replacing or rebuilding existing legacy infrastructures, followed by determining what set of technologies agencies need.



IT Professionals find vendor determination more challenging than program managers

55% vs 44%

Defense agencies find the following more challenging than civilian agencies

COSTLY INVESTMENT

61% vs 37%

LACK OF INTERNAL RESOURCES TO MANAGE

45% vs 26%

"When some agencies still have data on mainframes or legacy systems, it's a big challenge. Agencies know they can't bolt on zero trust, so they must decide to rebuild or replace systems. That requires additional spending on top of investing in zero trust. Agencies have to make some hard decisions."

John Sahlin, Ph.D.
Director, Cyber Solutions, Defense
GDIT

WHAT THIS MEANS

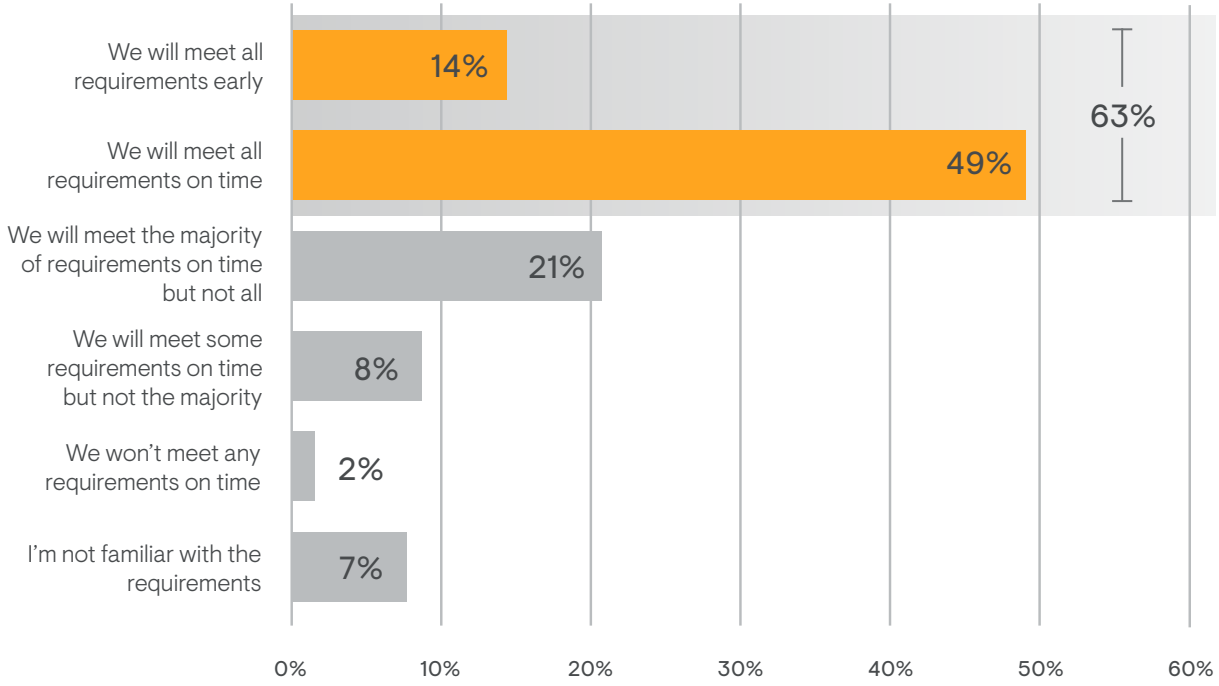
Moving to zero trust means starting from the ground up, requiring a significant investment – including replacing or rebuilding legacy infrastructure and mission systems built on "implicit trust." Legacy systems across the government rely on this model, which has, in many cases, proven unreliable and allowed malicious actors to gain access to systems and move around without granular controls offered by zero trust in place. Agencies should focus on introducing zero trust gradually by starting with areas that need the most attention and deliver quick wins. Agencies will have opportunities to budget for other investments they can't source from existing funding and should include those in their strategies.

Improving collaboration between mission owners and IT teams will ensure stronger alignment between the mission and cybersecurity technology implementation, making it easier to know which mission-enabling tools to select. In addition, it's important for agencies to partner closely with third parties to address these cyber challenges and implement successful zero trust strategies.

Meeting the 2024 Deadline

The executive order set a deadline for agencies to achieve certain zero trust goals set by the OMB by the end of the 2024 fiscal year. About two-thirds of agencies expect to meet those goals on time or ahead of the 2024 deadline. Another 21% will come close. Beyond 2024, agencies will need to continue to adopt the CISA Zero Trust Maturity Model.

Timeline to Meeting Executive Order Requirements



WHAT THIS MEANS

Although there are deadlines, this is not a race. As the January 2022 memo from OMB notes, this is "a journey for the federal government, and there will be agile learning and adjustments along the way." What's important is that agencies develop and effectively implement strategies that are right for their missions and the people they serve. For many agencies, those strategies require starting from scratch, but time and budgets don't always allow for that. If this is the case, agencies need to focus on making incremental improvements through their zero trust strategies.

- Optimize current infrastructure configurations
- Automate repetitive tasks
- Automate privilege review and sunset aging credentials
- Discover how users are accessing applications and services
- Implement explicit permit policies
- Develop automation scripts for security information and event management (SIEM) and security orchestration and response (SOAR)

GDIT

Market Connections®
Research you can act on.

Investment Priorities

Investment priorities over the next year track with a compliance-focused approach to implementing zero trust: nearly all respondents note their top investment priorities are device protection (92%) and cloud services (90%).

DEVICE PROTECTION

9 in 10

92%

CLOUD

9 in 10

90%

ICAM

3 in 4

76%

SASE

6 in 10

60%

MICRO-SEGMENTATION

1/2

51%

AI

1/2

47%

WHAT THIS MEANS

The investments that would most benefit mission efforts lag behind the other priorities: Secure Access Service Edge (SASE) (60%), micro-segmentation (51%), and AI (47%). For example, micro-segmentation reduces the attack surface and AI facilitates granular data protection, both of which are critical to enabling the mission.

There are also several challenges standing in the way of agencies determining their mission-focused investment priorities. Half the respondents are having trouble identifying what technologies they need, 48% stated a lack of IT staff, and 46% are concerned about costs. These responses show the challenges agencies face with accelerating zero trust progress and deciding what to prioritize first.

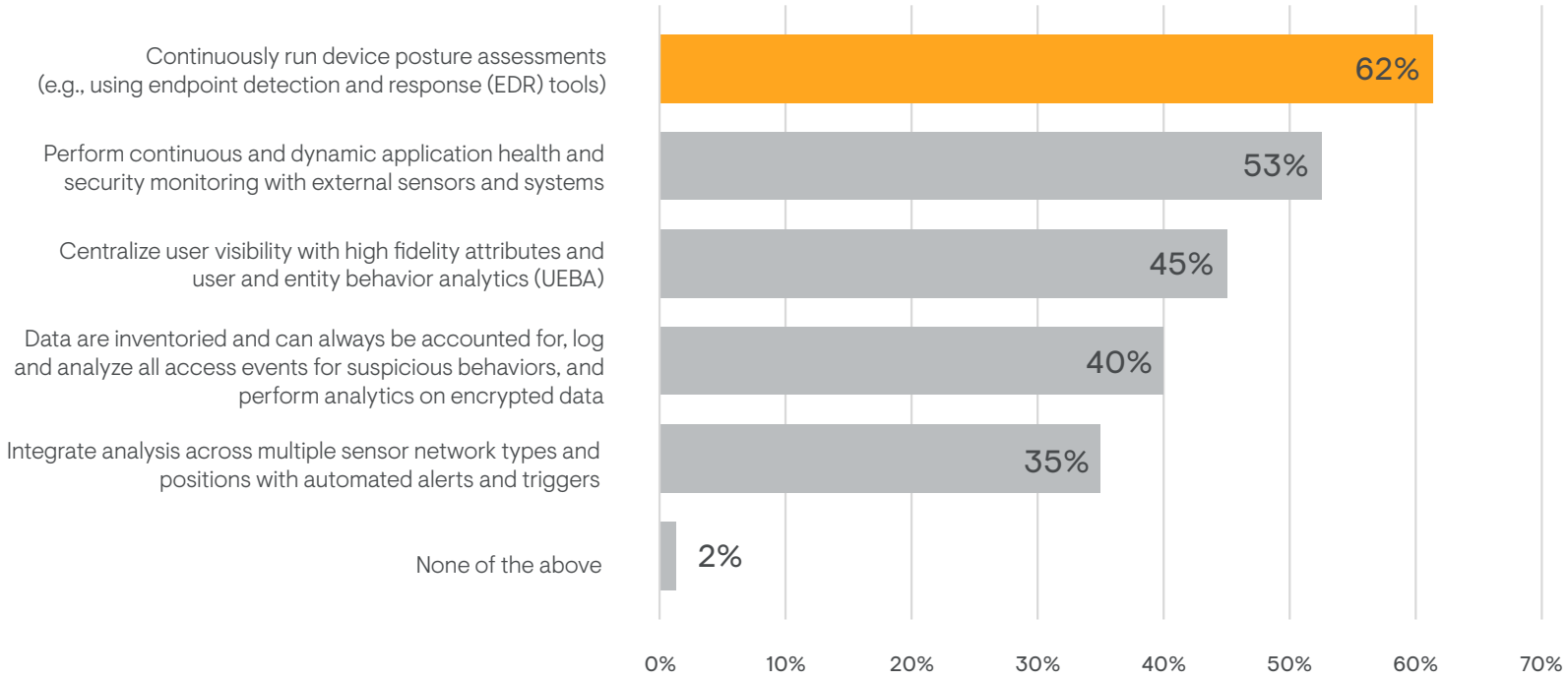
GDIT

Market Connections®
Research you can act on.

Achieving Visibility and Analytics Capabilities

Six in ten believe they will be able to continuously run device posture assessments (e.g., using endpoint detection and response tools) by the end of FY24.

Visibility and Analytics Capabilities Agencies Expect to Achieve by the End of FY2024



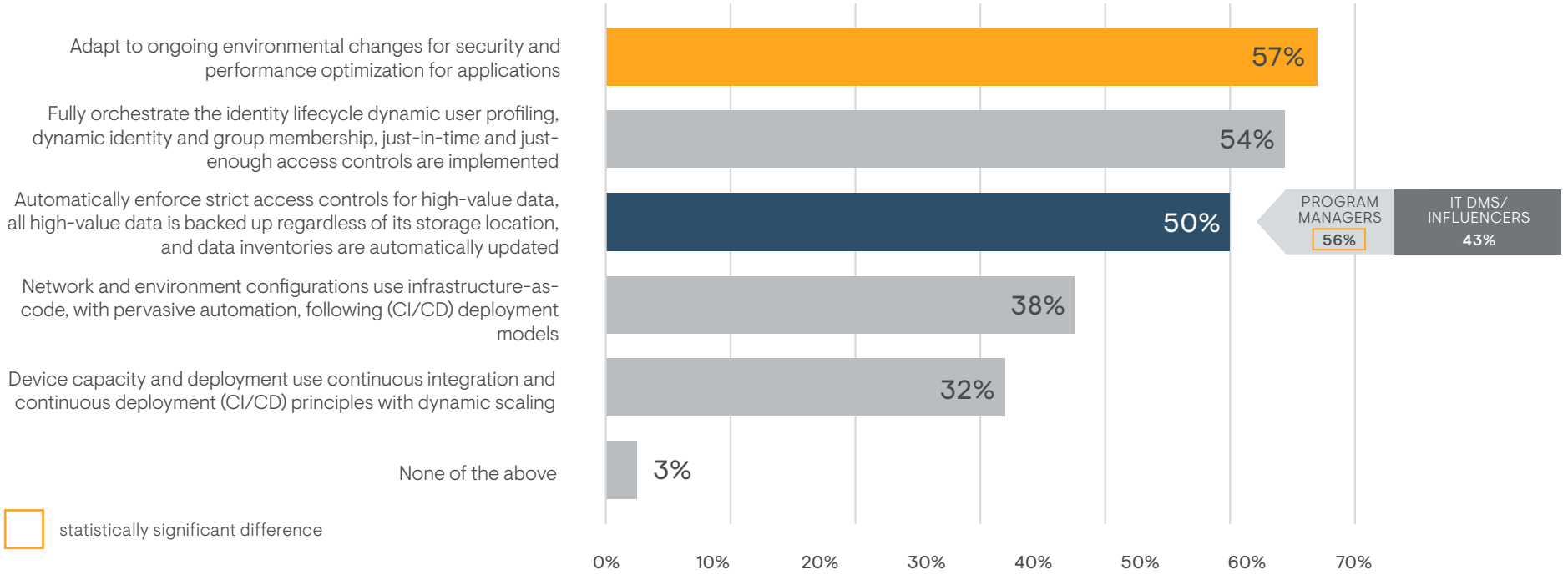
WHAT THIS MEANS

Analytics platforms consolidate data from multiple sources to provide visibility into agencies' environments. This visibility helps develop insight, contextual understanding that enables threat detection, and, ultimately, responses to those threats. A core component of zero trust, analytics are key to enabling SOAR capabilities. The use of EDR tools will allow increased visibility and analytics and enable increased visibility into device pillar posture.

Achieving Automation and Orchestration Capabilities

Over half believe they will be able to adapt to ongoing environmental changes for security and performance optimization for applications by the end of FY24. More program managers than IT respondents feel their agency will be able to automatically enforce strict access controls for high-value data, all high-value data will be backed up regardless of its storage location, and data inventories will be automatically updated..

Automation and Orchestration Capabilities Agencies Expect to Achieve by the End of FY2024



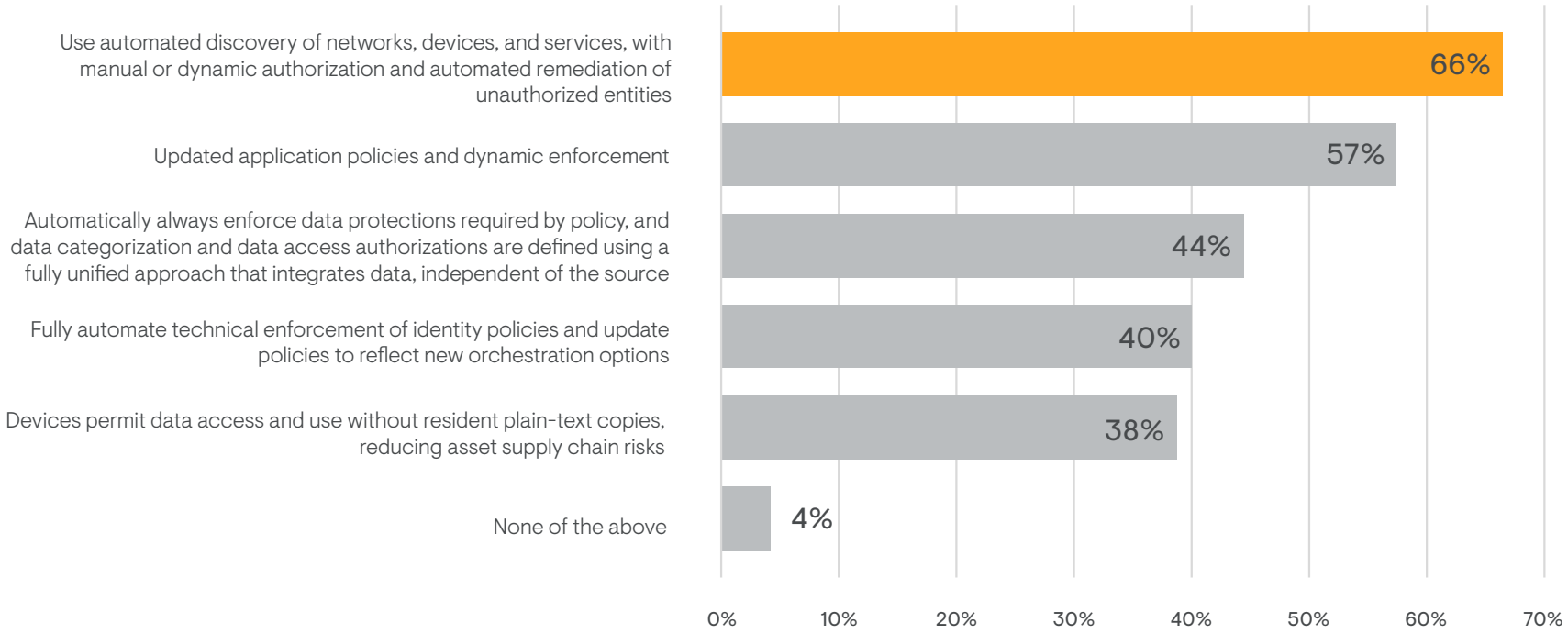
WHAT THIS MEANS

Digital enterprises move quickly, and the threat environment continues to evolve, making it impossible for manual security processes to keep pace. Embracing automation and orchestration to orchestrate processes and automate tasks performed by security teams will save time and improve productivity. Many agencies have realized that they need to automate to achieve a higher level of zero trust maturity to secure their users, devices, networks, application workloads, and data. As technology increases, data increases, and threats increase. The ability to scale leveraging automation will be paramount for implementation of zero trust.

Achieving Governance Capabilities

Two-thirds believe their agency will be able to use automated discovery of networks, devices, and services with manual or dynamic authorization and automated remediation of unauthorized entities by the end of FY24.

Governance Capabilities Agencies Expect to Achieve by the End of FY2024



WHAT THIS MEANS

As the emphasis on increasing enterprise visibility through identification of assets becomes more important agencies are finding that having technologies that automate the discovery of networks, devices, and services with the ability to provide automatic authorization and remediation will be key followed by more automated dynamic policy enforcement.

NEXT STEPS

Focus IT Investments On Mission Outcomes

Enabling the mission is, and always will be, the primary concern for federal agencies. The data shows the majority (52%) are using the CISA Zero Trust Maturity Model to establish strategies, indicating they are focused on maturity beyond OMB's zero trust memo. The value of zero trust is ensuring the right users have the right access to the right resources at the right time, however, respondents consistently put data and application layer security at the bottom of the list of priorities.

In developing and implementing zero trust strategies, agencies must be compliant, but checking the box is not good enough. Agencies need to ensure that their zero trust strategy maps to their mission. This means investing in technologies that will prepare them for emerging cyber threats, which might not have been considered under current standards, without creating new obstacles for mission owners.

Shifting the Compliance Focus

In today's environment, there are mountains of guidelines and standards to which agencies must comply—it's hard for them not to be purely compliance driven. The investments agencies are making now are important to achieving their zero trust strategies, but other technologies can support compliance requirements and protect against emerging and unknown threats. To help focus on the mission value of IT—while still meeting compliance requirements—there are several steps agencies can take.

Focus on executable outcomes that help move you down the road.

For many agencies, the biggest question is "Where do we begin?" Agencies need to understand where their organization fits within the cybersecurity threat landscape. The critical first step is to identify your digital assets and how they relate to the agency's mission—not every asset has equal impact. Ask yourself, "How does compromising this asset affect my mission outcomes?" This will help prioritize the type of security controls you need to apply to each asset.

Understand the guidance and how it applies to the agency mission.

Mere compliance is not enough, which is why an IT-centric or compliance-driven approach is not likely to meet the mission need. Agencies must have their IT departments partner with the mission owners to understand the impacts of data and services on each mission and ask, "How can I make the mission most effective and efficient through the lens of zero trust maturity?"

Start with where you are.

It's better to build a zero trust system from the ground up, but that isn't always possible. Determine, based on the mission, which projects optimize the limited investment dollars, provide the greatest progress, and protect the mission outcomes. It is possible to work with technologies and existing investments—finding a way to improve security while keeping traditional implicit trust models when that's the only option. Starting with a pilot and moving legacy systems into the new environment one at a time is a solution when budgets are tight.

After assessing the above three steps, prioritize your investments and technologies.

Focus on transitioning from a cost-based accounting project model to a value-driven approach and delivering value early through quick win projects, such as focusing on a high-value system or implementing a zero trust technology gap, that you can source within current agency funding. After demonstrating value early, align future IT investments to the mission outcomes they deliver.

A Marathon, Not a Sprint

With all the guidance and mandates, combined with the ever-changing cyber landscape, knowing which investment priorities will meet zero trust requirements across each CISA pillar, and how they integrate, is daunting. That is, unless you simply start with where you are today.

1

Discovery.

Understand what you have today and what your capabilities are. Look at how your team accesses systems, data, and services to execute the mission. Model current behavior and then build a plan for improving zero trust maturity.

2

Executable Roadmap.

Identify a set of executable projects that help you advance toward a more mature zero trust environment.

3

Quick Wins.

You can deliver rapid progress simply by optimizing your current infrastructure — start by identifying which applications and services can transition to zero trust through configuration changes and policy updates.

4

Prioritize Investments.

Rather than focusing on a particular zero trust pillar, identify which projects focus on improving mission effectiveness.

And above all else, remember that the primary value of zero trust is, and will continue to be, enabling mission objectives by providing data and services to the people who need them when they need them.

GENERAL DYNAMICS
Information Technology

About General Dynamics Information Technology

As a trusted systems integrator for more than 50 years, General Dynamics Information Technology is a leader in cybersecurity, supporting defense, intelligence, federal, and civilian agencies at the digital frontlines. GDIT delivers advanced cyber solutions at the highest security levels supporting the most sensitive missions by bringing together more than 30 leading commercial technology partners to address agencies' unique challenges. GDIT offers agencies a comprehensive, integrated ecosystem of capabilities from identity management, to endpoint security, to artificial intelligence that provide a holistic defense against cyber threats and help agencies achieve optimal zero trust maturity. For more information, visit: www.gdit.com/cyber.

CONTACT

GENERAL INQUIRIES
Christopher Aiello
Senior Marketing Manager
GDIT
Email: christopher.aiello@gdit.com

MEDIA INQUIRIES
Jay Srinivasan
Senior Public Relations Manager
GDIT
Email: jayendran.srinivasan@gdit.com

Market Connections®
Research you can act on.

About Market Connections

Market Connections, a portfolio platform of GovExec, 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.

CONTACT

Elizabeth Lowery
Director of Research Services
Market Connections
Email: elowery@govexec.com