# Your Roadmap to Zero Trust Success in the Cloud

## MARKET TRENDS REPORT

govloop

E-INFOSOL LLC
INNOVATIVE SECURE IT SERVICES & GREEN SOLUTIONS

aws

# Executive Summary

Federal agencies are under pressure to adopt a zero-trust approach to cybersecurity, and many are struggling to get there.

A May 2021 executive order on cybersecurity made zero trust a mandate for federal agencies, and a January 2022 White House memorandum laid out a formal strategy. But beyond mere compliance, there's a practical mandate for zero trust as well.

Given the complexity of the IT infrastructure in federal agencies and the increasingly adversarial cyber environment, agencies need a more robust way to secure data and systems as they move toward modernized IT environments. While the adoption of cloud infrastructure makes security easier in some respects, agencies will still need to leverage a zero trust approach as they seek to map their cloud security strategies back to the core technology concepts that they already apply.

The urgency is high, but for many federal agencies, there's no clear path to zero trust.

The White House memo recognizes the challenge. "Transitioning to a zero trust architecture will not be a quick or easy task for an enterprise as complex and technologically diverse as the Federal Government," it notes. "This process will be a journey … and there will be learning and adjustments along the way as agencies adapt to new practices and technologies."

To explore how agencies can ease the transition, GovLoop collaborated on this report with E-INFOSOL, a provider of cloud computing, virtualization, cyber security, software development and data services in support of government.

We'll discuss some of the challenges on the road to zero trust. We'll look at the means by which agencies can move forward, and lay out some key best practices in support of an emerging zero-trust architecture.

# By The Numbers

According to Gartner, the number of large enterprises with a comprehensive, mature and measurable zero-trust program in place will rise sharply over the next two years:


A 2022 survey by the Cloud Security Alliance found that zero trust increasingly is playing a strategic role in large organizations. Key findings include:

**80%** of C-level executives have zero trust as a priority for their organizations.

**94%** are in the process of implementing zero trust strategies.

**77%** are increasing their spending on zero trust over the next 12 months.

***But the benefits of zero trust are clear:***

# 87%

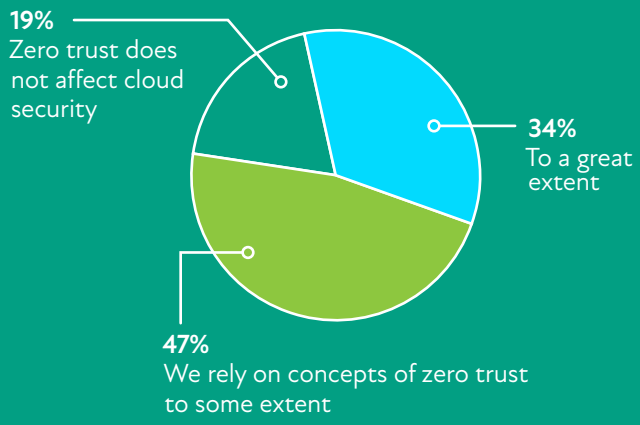
of security professionals who have adopted a zero-trust approach have found that it improved productivity.

***"In essence, a zero trust architecture allows users full access but only to the bare minimum they need to perform their jobs."***

- Executive Order on Improving the Nation's Cybersecurity

**Zero trust is an important part of cloud security in most organizations:**

To what extent does zero-trust security shape your cloud security strategy?




But the obstacles to zero trust are numerous, the survey found. Between 29% and 35% of respondents identified the following areas as challenges:

**34% - Identity and access management**

**31% - Data flow management**

**31% - Network security**

**30% - Asset management**

**29% - Application dependencies**

**29% - Governance and policy**

**29% - Behavior monitoring**

**29% - Endpoint/device security**

# How to Overcome Cloud Security Stumbling Blocks

## The Challenge: Outdated Solutions, Competing Priorities

A number of key challenges emerge as agencies seek to implement cloud services that meet zero-trust requirements.

- **Technical debt:** Identity and access are key safeguards in a zero-trust network architecture. As defined by the National Institute of Standards and Technology (NIST), zero trust "uses the identity of actors as the key component of policy creation."

  That means agencies need a unified way to address identity and access management (IAM). Yet many are saddled with legacy technology that doesn't support a modernized approach. "While agencies may have centralized identity and access management, the use of enterprise identities must be enforced," said Robert Szot, Vice President of Cloud Services at E-INFOSOL.

- **Competing priorities:** Zero trust isn't the only agenda item for federal IT teams. They're busy trying to build new applications; they're looking for ways to elevate the constituent experience; they're launching artificial intelligence initiatives to improve efficiency.

  "They are facing a lot of competing priorities, with limited manpower," said Chad Thomas, Chief Information Officer at E-INFOSOL. "Their job is to get new systems and applications out the door, and they don't necessarily have the time they need to devote to zero trust."

- **Lack of key skills:** Ensuring security in the cloud environment requires new and different skills. While cloud shifts much of the security burden onto the cloud provider, agencies still have some responsibility, and a new environment will require an approach to cyber that goes beyond what's required in an on premises-based architecture. Many agencies discover they do not have the needed skill sets on hand.

  "For agencies working in the cloud environment, pursuing cloud modernization, there is a gap when it comes to the skills needed to design and architect for zero trust," Szot said. That gap may slow an agency's ability to bring higher-level security to its cloud implementations.

## The Solution: Accelerating Zero Trust

Talent gaps and competing priorities suggest that federal IT teams may need to bring in outside help in order to address the technical debt that gets in the way of zero-trust adoption. Those looking to accelerate their zero-trust journey can partner with a third-party IT consultancy for security assessments, prioritization and key implementation services in order to achieve a modernized security footing. Outside experts can help:

- **Identify the gaps:** An outside consultant can perform an initial assessment to identify underlying gaps in the existing security apparatus. Such an assessment can help chart a path toward improvement, as agencies seek to translate zero-trust guidance into practical action.

  "There may be gaps in policy, gaps in procedure, as well as in the technology supporting cybersecurity," Thomas said. In zero trust, all those need to be in alignment. An initial assessment can highlight the potential weak points and lay out a program of remediation.

- **Establish priorities:** Based on the results of the initial assessment, the agency can leverage the consultants' expertise to prioritize its plan of action. With IT teams pulled in many different directions, this effort to define priorities is a key driver of effective action on zero trust. The result is a roadmap that will help guide the agency's zero-trust efforts in a focused way.

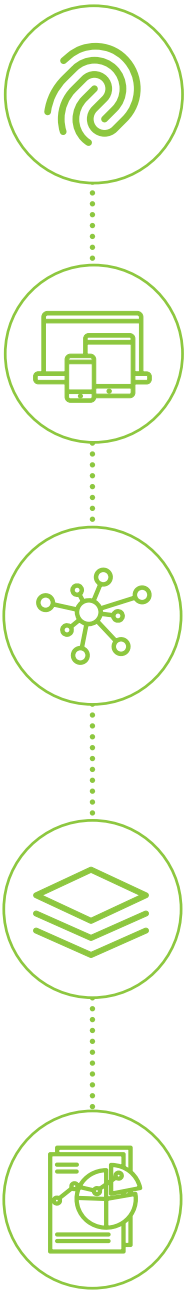
  "With budgetary and staffing constraints, you can't do everything at once, so you need to know which vulnerabilities or gaps you want to tackle first," Szot said. "You need to prioritize the highest-risk deficiencies first, as part of a larger roadmap."

- **Leverage automation:** As agencies bring to life their zero-trust plans, they'll want expert guidance in order to implement automated controls and processes.

  "With automation, you can spend less time worrying about the infrastructure and the security guardrails," Thomas said. "Automation helps ensure agencies aren't perpetuating bad security practices as they migrate to new architectures."

# Best Practices in Zero Trust

Security best practices on the path to modernization should focus on the five pillars of a zero-trust framework:



**Identity:** Government needs to think in new ways about identity and access management in the cloud. Leaders need to look beyond the fragmented and siloed solutions of the past, and work toward a more cohesive and unified approach.

"Agencies need to focus on identity consolidation, identity federation," Szot said. "They need to know who's doing what, where. Identity is the new perimeter, and it is absolutely critical to securing infrastructure and applications."

**Devices:** In the modern IT environment, where remote work and Internet of Things devices play a big role, "it's critical to have full control of the endpoints," said Fredy Pesante, President, CEO and co-founder of E-INFOSOL.

Zero trust requires IT to think about the role that devices play, and to ensure they are being properly managed in support of the larger cybersecurity effort.

**Network:** In the past, network security meant hardening the outward-facing boundary. If IT could secure the perimeter, it could safeguard everything inside that wall. "That's no longer the case," Szot said.

Evolving vulnerabilities and threats require defense in depth, "not only providing boundary protection, but also delivering rules and policies at more granular levels," he said. "That means ensuring networks are managed and monitored holistically, rather than managed in a standalone way that may lack the needed protections."

**Application Workload:** As agencies move to the cloud, they need to rethink the security of their application development pipelines. They need to consider the software supply chain, as well as the security of their production environments.

"Where are you sourcing software from? Whether it is open source, or from third-party vendors, you need to do your due diligence before moving that software into production," Szot said. "There needs to be secure pipelines to build and manage applications, as well as to ensure those applications are only accessing data and other resources from a least-privilege perspective."

**Data:** When it comes to zero trust, data needs to be a central consideration: At the end of the day, that's what we are trying to secure.

"Agencies need to look at data access and data encryption, at rest and in transit," Thomas said. "They need to think about who is accessing the data. All of these are big concerns in support of effective zero trust."

***"Agencies need to look at data access and data encryption, at rest and in transit," Thomas said. "They need to think about who is accessing the data. All of these are big concerns in support of effective zero trust."***

# Case Study: Accelerating Zero Trust

For one federal agency, the pandemic threw zero-trust efforts into high gear.

With a massive surge in remote work, and a big boost in the utilization of cloud resources, IT leaders saw potential security gaps. "Their existing solutions lacked multifactor authentication, they lacked network monitoring and data protection," Szot said.

To supplement its in-house talent and ensure effective zero trust in the cloud environment, the agency brought in E-INFOSOL to assess the security situation, identify potential gaps and help implement a roadmap for change.

The E-INFOSOL team migrated a legacy remote-access solution to Amazon AppStream 2.0, AWS's fully managed application streaming service that provides users with instant access to their desktop applications from anywhere.

"We federated it with enterprise identity and multifactor authentication, and that became a new centrally managed, secure access point into the cloud environment for about 1,200 users. That solution was deployed in AWS GovCloud, multi-region, with high availability," Szot said.

The E-INFOSOL team performed the assessments to ensure the service itself was configured securely. And with the introduction of an AWS Network Firewall, E-INFOSOL enabled the agency to inspect network traffic across 130-plus virtual networks, a key security capability it had previously lacked.

With a successful zero-trust implementation, the agency was able to deliver cloud resources securely to its remote workers throughout the pandemic and beyond.

"It greatly reduced the risks involved with managing local user identities," Szot said. Overall, "we greatly increased the security posture of that environment."

## HOW E-INFOSOL AND AWS HELP

As an AWS Advanced Tier software engineering and cloud services partner, E-INFOSOL designs and builds secure solutions that accelerate federal efforts to achieve zero trust in the cloud. E-INFOSOL engineers collaborate with AWS Public Sector and National Security teams to build solutions that meet the security requirements for various federal network classification levels.

In addition to its presence in the AWS Marketplace, E-INFOSOL maintains an AWS private marketplace, through which it provides government users with a curated catalog of approved products. Here, government agencies can access a wide range of professional services in support of their zero-trust goals, including security assessments and implementation support.

With E-INFOSOL's AWS Private Marketplace enablement, agencies can unlock the full potential of AWS while maintaining complete control and compliance. They can simplify the procurement process and reduce the overhead of managing multiple vendors, saving time and accelerating deployment by accessing pre-approved software and services directly from the private marketplace.

# Conclusion

Federal agencies need to pivot to zero trust both to meet mandate, and to support their IT modernization efforts. However, many are struggling to get there. Internal talent gaps and competing priorities make it challenging for agencies to adjust systems and processes in support of the emerging security paradigm.

Agencies can build momentum by teaming with outside consultants, who can conduct the security assessments and prioritization needed to drive a shift to zero Trust. A third-party partner can also deliver the implementation services needed to make modernized security a reality, with availability of these services in a cloud marketplace, via a pre-approved catalog, helping to accelerate the Zero Trust journey.

## ABOUT


E-INFOSOL specializes in building modern and tailored solutions to support our customers' mission. As a people-first and mission-centric organization, we deliver Subject Matter Expertise (SME) in cloud computing, virtualization, cyber security, software development, and data services to our mission partners. We support the Intelligence Community, the Department of Defense, Federal Law Enforcement, Civilian Agencies, and the Private Sector.

Learn more:
https://www.e-infosol.com


Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform. Millions of customers, including government agencies, are using AWS to lower costs, become more agile, and innovate faster while powering infrastructure and providing reliable, mission critical services.

For more information please visit aws.amazon.com.


GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.


1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop