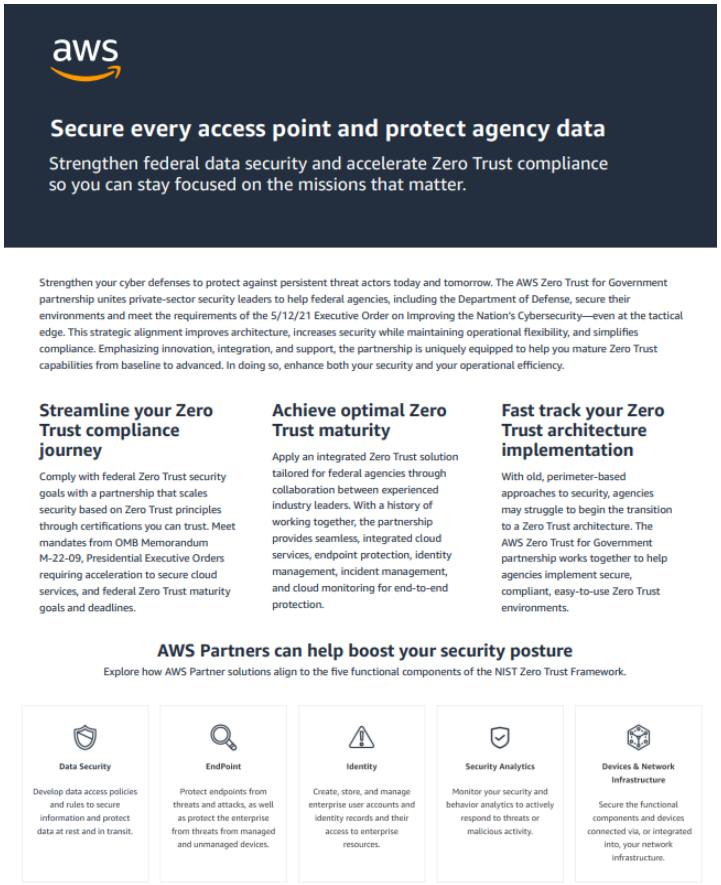
Secure every access point and protect agency data

Strengthen federal data security and accelerate Zero Trust compliance so you can stay focused on the missions that matter.



Secure every access point and protect agency data

Strengthen federal data security and accelerate Zero Trust compliance so you can stay focused on the missions that matter.

Strengthen your cyber defenses to protect against persistent threat actors today and tomorrow. The AWS Zero Trust for Government partnership unites private-sector security leaders to help federal agencies, including the Department of Defense, secure their environments and meet the requirements of the 5/12/21 Executive Order on Improving the Nation's Cybersecurity—even at the tactical edge. This strategic alignment improves architecture, increases security while maintaining operational flexibility, and simplifies compliance. Emphasizing innovation, integration, and support, the partnership is uniquely equipped to help you mature Zero Trust capabilities from baseline to advanced. In doing so, enhance both your security and your operational efficiency.

Streamline your Zero Trust compliance journey

Comply with federal Zero Trust security goals with a partnership that scales security based on Zero Trust principles through certifications you can trust. Meet mandates from OMB Memorandum M-22-09, Presidential Executive Orders requiring acceleration to secure cloud services, and federal Zero Trust maturity goals and deadlines.

Achieve optimal Zero Trust maturity

Apply an integrated Zero Trust solution tailored for federal agencies through collaboration between experienced industry leaders. With a history of working together, the partnership provides seamless, integrated cloud services, endpoint protection, identity management, incident management, and cloud monitoring for end-to-end protection.

Fast track your Zero Trust architecture implementation

With old, perimeter-based approaches to security, agencies may struggle to begin the transition to a Zero Trust architecture. The AWS Zero Trust for Government partnership works together to help agencies implement secure, compliant, easy-to-use Zero Trust environments.

AWS Partners can help boost your security posture

Explore how AWS Partner solutions align to the five functional components of the NIST Zero Trust Framework.

Data Security

Develop data access policies and rules to secure information and protect data at rest and in transit.

EndPoint

Protect endpoints from threats and attacks, as well as protect the enterprise from threats from managed and unmanaged devices.

Identity

Create, store, and manage enterprise user accounts and identity records and their access to enterprise resources.

Security Analytics

Monitor your security and behavior analytics to actively respond to threats or malicious activity.

Devices & Network Infrastructure

Secure the functional components and devices connected via, or integrated into, your network infrastructure.

carahsoft

For more information, contact Carahsoft or our reseller partners:
AWS@carahsoft.com | 888-662-2724

Thank you for downloading this AWS Resource! Carahsoft is the distributor for AWS public sector solutions available via GSA, NASPO, The Quilt and other contract vehicles.

To learn how to take the next step toward acquiring AWS's solutions, please check out the following resources and information:

For additional resources:
carah.io/AWS-Resources

For upcoming events:
carah.io/AWS-Events

For additional AWS solutions:
carah.io/AWS-Solutions

For additional public sector solutions:
carah.io/AWS.Solutions

To set up a meeting:
AWS@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/AWS-Contracts

Secure every access point and protect agency data

Strengthen federal data security and accelerate Zero Trust compliance so you can stay focused on the missions that matter.

Strengthen your cyber defenses to protect against persistent threat actors today and tomorrow. The AWS Zero Trust for Government partnership unites private-sector security leaders to help federal agencies, including the Department of Defense, secure their environments and meet the requirements of the 5/12/21 Executive Order on Improving the Nation's Cybersecurity—even at the tactical edge. This strategic alignment improves architecture, increases security while maintaining operational flexibility, and simplifies compliance. Emphasizing innovation, integration, and support, the partnership is uniquely equipped to help you mature Zero Trust capabilities from baseline to advanced. In doing so, enhance both your security and your operational efficiency.

Streamline your Zero Trust compliance journey

Comply with federal Zero Trust security goals with a partnership that scales security based on Zero Trust principles through certifications you can trust. Meet mandates from OMB Memorandum M-22-09, Presidential Executive Orders requiring acceleration to secure cloud services, and federal Zero Trust maturity goals and deadlines.

Achieve optimal Zero Trust maturity

Apply an integrated Zero Trust solution tailored for federal agencies through collaboration between experienced industry leaders. With a history of working together, the partnership provides seamless, integrated cloud services, endpoint protection, identity management, incident management, and cloud monitoring for end-to-end protection.

Fast track your Zero Trust architecture implementation

With old, perimeter-based approaches to security, agencies may struggle to begin the transition to a Zero Trust architecture. The AWS Zero Trust for Government partnership works together to help agencies implement secure, compliant, easy-to-use Zero Trust environments.

AWS Partners can help boost your security posture

Explore how AWS Partner solutions align to the five functional components of the NIST Zero Trust Framework.

Data Security

Develop data access policies and rules to secure information and protect data at rest and in transit.

EndPoint

Protect endpoints from threats and attacks, as well as protect the enterprise from threats from managed and unmanaged devices.

Identity

Create, store, and manage enterprise user accounts and identity records and their access to enterprise resources.

Security Analytics

Monitor your security and behavior analytics to actively respond to threats or malicious activity.

Devices & Network Infrastructure

Secure the functional components and devices connected via, or integrated into, your network infrastructure.

Streamline your Zero Trust Journey

Learn how CrowdStrike's approach to a frictionless Zero Trust journey can accelerate risk reduction and make the most of your existing technology investments.

Learn More

How to Protect Your Organization from Identity-Based Attacks

Organizations with gaps in their identity security are significantly more at risk of experiencing a compromise or breach. Find out what steps you can take to protect your organization from today's identity threats.

Learn More

Understanding Zero Trust with AWS & Splunk

Regardless of where you're at on your Zero Trust journey, Splunk can help you stay one step ahead of new and existing threats.

Learn More

An Architect's Guide to the Zscaler Zero Trust Exchange

Read the seven elements of highly successful Zero Trust architecture to learn how Zscaler's industry leading Zero Trust Exchange delivers fast, secure access for users, data, and workloads in AWS.

Learn More

Secure Zero Trust Data Security

XQ Zero Trust data platform delivers distributed file and structured data encryption across all trusted and untrusted environments. The patented technology suite provides decentralized data rights management and data loss prevention to separate environment and data access. XQ seamlessly interfaces with any technology.

Learn More

Secure access and permissions to all your systems

Koverse Data Platform (KDP) 4.0 introduces attribute-based access controls (ABAC) that allow customers to safely work with complex, sensitive information to power the most demanding analytics, data science, and AI use cases.

Learn More

Secure every access point and protect agency data