TCG
POSITIVELY DISTINCT®

Achieving NIST Zero Trust with AWS

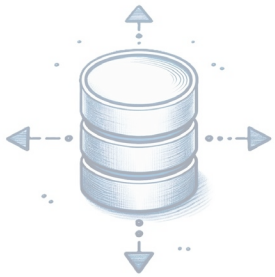
TCG's Reference Model

By Dr. Robert Buccigrossi,
TCG CTO

7348 GEORGIA AVENUE NW, WASHINGTON, DC 20012
INFO@TCG.COM | WWW.TCG.COM | 202-986-5533

Achieving NIST Zero Trust with AWS: TCG's Reference Model

Contents



Executive Summary

The purpose of this white paper is to present TCG's AWS reference model and guide for implementing a Zero Trust Architecture (ZTA) using AWS technologies in alignment with National Institute of Standards and Technology (NIST) 800-207 guidelines. While AWS estimates that 7,500 government agencies use its platform, there is a dearth of resources describing how to use AWS services to implement a NIST-compliant ZTA.

This paper focuses on helping federal agencies and other organizations understand the key components of ZTA, provides an overview of NIST 800-207 guidelines, and maps AWS services to these components.

TCG's model provide a comprehensive, phased approach to implementing Zero Trust that addresses the complexity and cost challenges associated with such a transformation. AWS's robust suite of security services seamlessly integrates with both modern and legacy systems, ensuring compliance with NIST 800-207 guidelines.

Additionally, AWS's advanced security features, continuous monitoring tools, and automated compliance checks provide the necessary infrastructure to maintain a secure and resilient environment, ultimately enhancing an agency's ability to defend against evolving cyber threats.

Introduction

Cybersecurity Challenges to Federal Agencies

The cybersecurity landscape for federal agencies has evolved dramatically, driven by the increasing complexity of IT environments and the proliferation of cloud services, remote workforces, and sophisticated cyber threats. Traditional perimeter defenses are no longer sufficient to protect against advanced persistent threats (APTs), insider threats, and zero-day vulnerabilities.

The rise of cloud computing, mobile workforces, bring your own device (BYOD) policies, and the Internet of Things (IoT) has blurred the network perimeter, making it easier for attackers to leverage sophisticated techniques to breach defenses and move laterally within networks.

TCG's model provides a comprehensive, phased approach to implementing Zero Trust that addresses the complexity and cost challenges associated with such a transformation.

Introduction to Zero Trust Architecture

ZTA represents a paradigm shift in cybersecurity, moving away from traditional perimeter-based security models to a comprehensive approach that assumes no implicit trust within a network. Instead, ZTA continuously verifies and validates every request for access to data and resources, regardless of the source. It relies on strict identity verification, granular access controls, and continuous monitoring to protect organizational assets.

The core principle of Zero Trust is "never trust, always verify," ensuring that only authenticated and authorized users and devices gain access to critical systems and data. This approach significantly reduces the attack surface and minimizes the risk of data breaches and unauthorized access.

IT RISKS By the Numbers

Every **39** seconds a single public computer on the Internet has a hacking attempt.

Source: University of Maryland

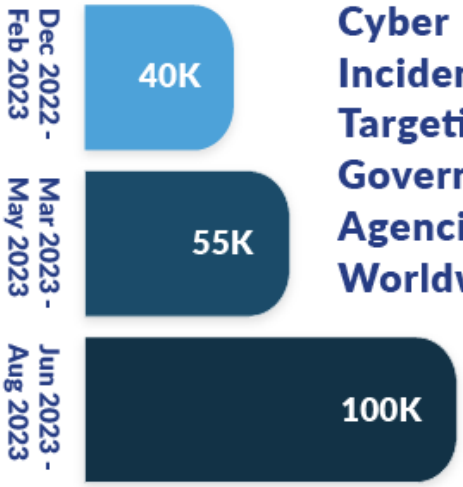
of organizations worldwide have either fully or partially implemented a zero-trust strategy.

Source: Gartner

If the Cyber Economy were a country, it would have an **$8T Annual GDP**, making it the 3rd largest economy in the world.

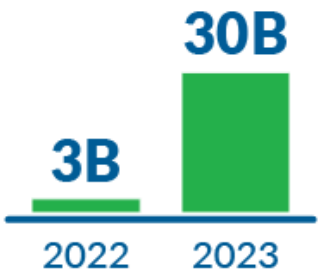
Source: Cybersecurity Ventures

USA	China	Cyber Economy	Germany	Japan
$27T	$17.8T	$8T	$4.4T	$4.2T



Cyber Incidents Targeting Government Agencies Worldwide

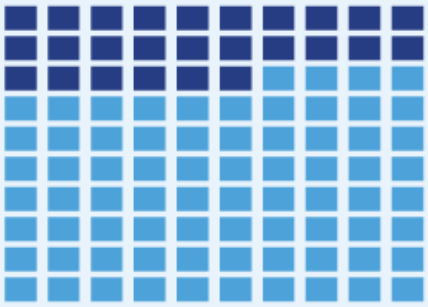
Source: Statistica



Password Attacks per Month

Source: Microsoft

100 reported cases of public data exposure in 2023



Up from **74 cases** in 2022

These incidents impacted **15 million** people.

Source: Statistica

Key Requirements for Federal Agencies

The importance of ZTA in today's cybersecurity landscape is underscored by Executive Order 14028, "Improving the Nation's Cybersecurity," issued on May 12, 2021. This Executive Order mandates federal agencies to enhance their cybersecurity measures, including adopting ZTA wherever practicable. In response to this order, NIST Special Publication 800-207 provides comprehensive guidelines for implementing ZTA. It defines the logical components, core principles, and various deployment scenarios that organizations can adopt to enhance their cybersecurity posture.

For federal agencies, adherence to NIST 800-207 is critical as it aligns with mandates for stringent data protection and cybersecurity resilience. The publication emphasizes continuous authentication, dynamic policy enforcement, and real-time monitoring, which are crucial for safeguarding sensitive government information and ensuring compliance with federal security standards.

The Perimeter is Breached

Traditionally, organizations relied on perimeter-based security models, that created a strong defensive boundary around the network. This approach, often described as the "castle and moat" model, assumed that threats were primarily external, and once inside the network, users and devices were trusted by default.

Firewalls, intrusion detection systems (IDS), and antivirus solutions formed the core of this perimeter defense strategy**. However, the perimeter-based model has proven inadequate in addressing modern cybersecurity challenges**.

NIST SP 800-207 Guidelines

NIST provides a comprehensive framework for implementing a ZTA, focusing on continuous verification and strict access controls. The core components of ZTA as defined by NIST 800-207 include:

Core Component	Description
Policy Enforcement Point (PEP)	The PEP is responsible for enabling, monitoring, and terminating connections between users and enterprise resources. It acts as the gatekeeper, enforcing access policies based on decisions made by the Policy Engine and executed by the Policy Administrator.
Policy Administrator (PA)	The PA manages the configuration of PEPs and ensures that the appropriate access policies are enforced. It generates session-specific credentials and oversees the establishment and termination of connections.
Policy Engine (PE)	The PE is the central decision-making component that evaluates access requests against enterprise policies and threat intelligence. It uses a trust algorithm to determine whether to grant or deny access based on various contextual factors.
Security Policies & Threat Intelligence	These components provide the rules and contextual information used by the PE to make informed access decisions. They include data access policies, identity attributes, threat intelligence feeds, and compliance requirements.
Continuous Diagnostics & Mitigation (CDM)	The CDM system provides real-time information on the security posture of enterprise assets. It feeds data into the PE, enabling dynamic policy adjustments based on the current state of devices and networks.

The NIST 800-207 guidelines highlight the importance of continuous monitoring, dynamic policy enforcement, and least-privilege access principles. By integrating these components, organizations can create a robust and adaptive security framework that minimizes the risk of unauthorized access and enhances overall cybersecurity resilience.

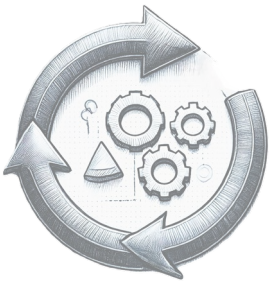
AWS and Zero Trust Architecture

Addressing Zero Trust Challenges with AWS

Using native AWS services can significantly address the challenges federal agencies face in adopting ZTA, particularly when dealing with legacy systems. AWS offers a comprehensive suite of security services and tools designed to integrate seamlessly with both modern and legacy infrastructures.

This integration capability simplifies the process of retrofitting legacy systems to comply with Zero Trust principles. For instance, AWS Identity and Access Management (IAM) and AWS Single Sign-On (SSO) can provide robust identity verification and access control, even for legacy applications that may not natively support modern authentication protocols.

An iterative approach allows agencies to transition to Zero Trust incrementally, mitigating the risk of a monolithic, disruptive transition and providing a faster return on investment.



Additionally, AWS Transit Gateway and AWS Direct Connect can help create secure, scalable network architectures that facilitate the implementation of Zero Trust principles across hybrid environments.

One of the primary benefits of leveraging AWS for Zero Trust is the ability to adopt services iteratively. This iterative approach allows agencies to transition to Zero Trust incrementally, mitigating the risk of a monolithic, disruptive transition and providing a faster return on investment.

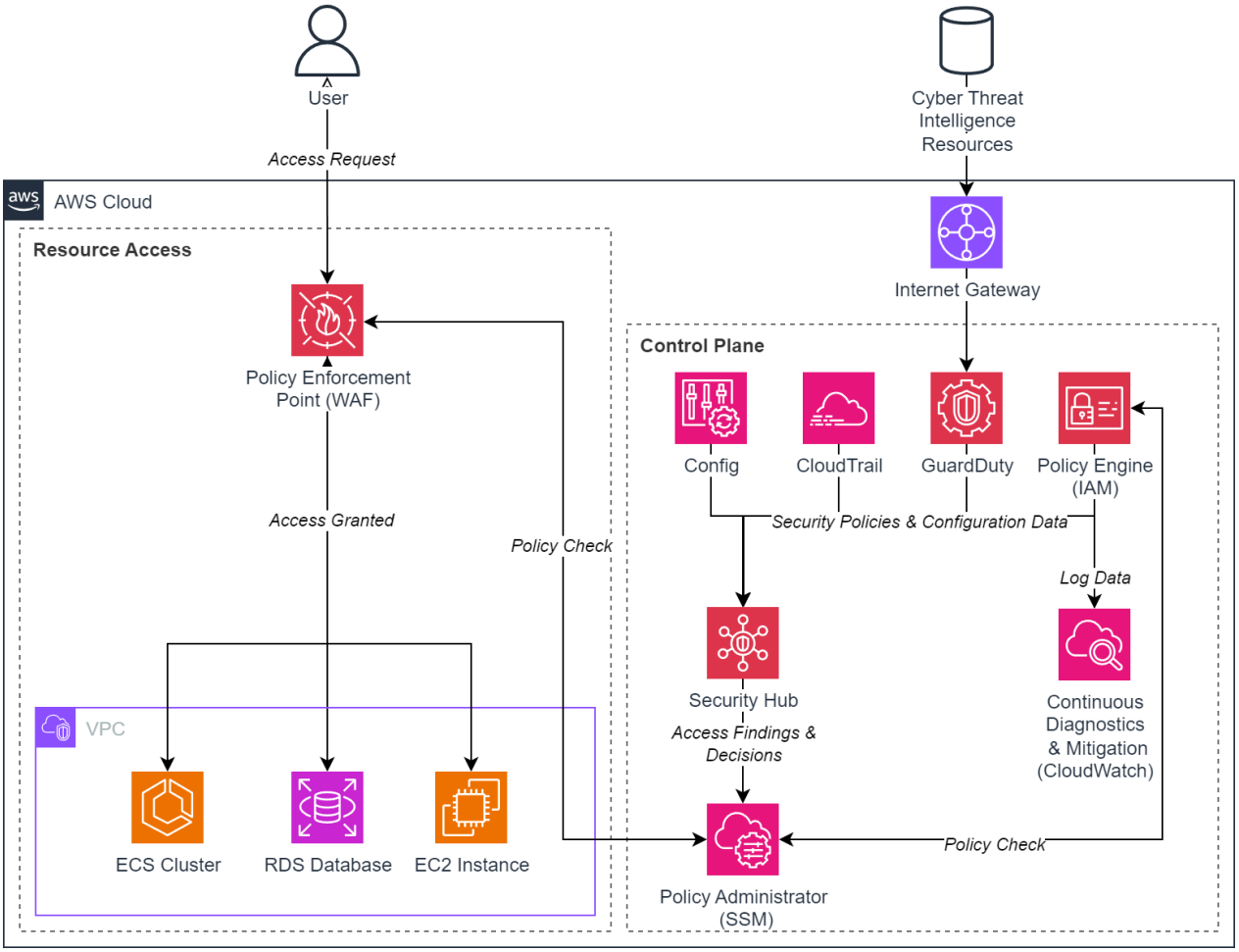
Agencies can start by implementing foundational services such as AWS CloudTrail for logging and monitoring, AWS GuardDuty for threat detection, and AWS Security Hub for centralized security management. Over time, additional layers of security can be added, such as AWS Network Firewall for network segmentation and AWS Secrets Manager for secure management of credentials. This phased adoption enables agencies to continuously enhance their security posture without overhauling their entire infrastructure at once.

AWS and Zero Trust Architecture (continued)

Challenge	How AWS Addresses ZTA Challenges
Integration with Legacy Systems	AWS IAM and AWS SSO enable robust identity verification and access control for legacy applications, simplifying integration.
Disruptive Transition	AWS allows for iterative implementation of Zero Trust principles, reducing the risk of disruptive transitions and providing quicker ROI.
Cost and Complexity	Native AWS services like AWS CloudTrail, AWS GuardDuty, and AWS Security Hub streamline security management and reduce the complexity of Zero Trust implementation.
Compliance and Regulation	AWS's compliance framework ensures alignment with federal regulations, simplifying the process of achieving and maintaining compliance.
Interoperability	AWS services are designed to work seamlessly together, ensuring smooth integration across on-premises, cloud, and hybrid environments.
Continuous Monitoring	AWS CloudWatch and AWS Config provide continuous monitoring and automated compliance checks, ensuring real-time visibility into the security posture.
Threat Detection	AWS GuardDuty and AWS Security Hub offer advanced threat detection and centralized security management.
Data Protection	AWS KMS and AWS Secrets Manager provide robust encryption and secure management of sensitive data.
Network Security	AWS Network Firewall and AWS Transit Gateway facilitate secure, scalable network architectures.
Scalability	AWS services can scale to meet the needs of federal agencies, ensuring that security measures can grow with the organization.

TCG's AWS Zero Trust Model

Implementing ZTA in AWS involves integrating various AWS services to create a secure and resilient environment. This model leverages AWS's robust security capabilities to meet the requirements of NIST 800-207, ensuring continuous authentication, granular access control, and comprehensive monitoring. The following diagram illustrates how AWS services can be mapped to the core components of a Zero Trust Architecture: Policy Engine (PE), Policy Administrator (PA), Policy Enforcement Point (PEP), and Continuous Diagnostics and Mitigation (CDM).



TCG's AWS Zero Trust Model (continued)

In this model, the Policy Engine (PE) is represented by AWS Identity and Access Management (IAM) and AWS Security Hub, which aggregate and prioritize security findings to inform access decisions. The Policy Administrator (PA) leverages AWS Systems Manager (SSM) to manage configurations, state information, and automate operational tasks. Continuous Diagnostics and Mitigation (CDM) is achieved through AWS CloudWatch, which monitors resources and applications, triggering alerts and automations as necessary.

TCG's model is scalable, allowing security measures to grow with your organization without significant additional investments.

The Policy Enforcement Point (PEP) uses AWS Web Application Firewall (WAF) to protect web applications and APIs by enforcing access control policies. AWS Network Firewall further enhances network-level enforcement, ensuring that only authorized traffic is allowed. AWS GuardDuty provides advanced threat detection and continuous security monitoring, feeding critical threat intelligence into AWS Security Hub.

Through AWS infrastructure, TCG's model is scalable, allowing security measures to grow with the organization without significant additional investments. While supporting the NIST SP 800-207 standard, it supports an incremental adoption approach, enabling agencies to implement Zero Trust principles iteratively, mitigating the risk of disruptive transitions and ensuring quicker returns on investment (ROI).

Furthermore, it enhances threat detection and response through advanced services like AWS GuardDuty and centralized security management with AWS Security Hub. Robust data protection is ensured with AWS KMS for encryption and AWS Secrets Manager for secure data management. The cost efficiency of AWS's pay-as-you-go pricing model helps federal agencies optimize their security expenditures. **These advantages make TCG's AWS Model an effective and efficient solution for implementing a NIST ZTA, significantly enhancing cybersecurity resilience against evolving threats.**

Conclusion

Future of ZTA in Federal Agencies

The adoption of Zero Trust practices is not just a strategic advantage but a necessity for federal agencies in the current cybersecurity landscape. Executive Order 14028, "Improving the Nation's Cybersecurity," underscores the urgency for federal agencies to enhance their cybersecurity measures, including the adoption of Zero Trust principles. As cyber threats continue to evolve, the implementation of ZTA will become increasingly critical in protecting sensitive government information and maintaining national security. The future of ZTA in federal agencies will likely involve continuous evolution and integration of advanced security technologies, driven by both regulatory requirements and the need to stay ahead of sophisticated cyber adversaries.

We encourage federal agencies to embark on their Zero Trust journey with AWS, leveraging the phased approach outlined in this white paper. By starting with a thorough assessment and planning phase, agencies can build a solid foundation for implementing Zero Trust principles. AWS's extensive suite of security services provides the tools necessary to secure data, manage identities, enhance network security, and continuously monitor and mitigate threats. The iterative adoption of these services allows for a smooth transition, minimizing disruption while progressively enhancing the security posture. Now is the time for federal agencies to take decisive action, adopt Zero Trust Architecture, and fortify their defenses against ever-evolving cyber threats. By partnering with TCG and AWS, agencies can ensure they are well-equipped to meet the demands of the modern cybersecurity landscape.

To explore how this solution may fit your agency's needs, please contact:

Michael Drescher, Executive Director of Growth

michael.drescher@tcg.com | 703-969-7010

To inquire about the technical aspects of our proposed solution, please contact:

Dr. Robert Buccigrossi, Chief Technology Officer

robert.buccigrossi@tcg.com | 202-742-8473