

Zero Trust journey in the Government & Public Sector

Supporting your zero trust architecture transformation journey

What is Zero Trust and Zero Trust Architecture?

Zero Trust is a security model that moves from static, network-based cyber defenses to a continuously validated security configuration across 5 key pillars: identity, device, network/environment, application workload and data. Zero Trust enforces the cybersecurity concept of "never trust, always verify."

Zero Trust Architecture (ZTA) is a security framework that defines how Zero Trust services, including network infrastructure (physical and virtual), access workflows and operational policies, are structured to enable a Zero Trust security model.

The need for Zero Trust in the Government & Public Sector

Increased risk

- More sophisticated phishing, malware, ransomware and extortion threats
- Sharp increase in supply chain attacks
- Widespread compromise of credentials

Regulatory requirements

- Executive Order (EO) 14028 required agencies to create a ZTA implementation plan.
- ► M-22-09 requires agencies to follow a prescriptive timeline to achieve specific ZTA security goals by the end of FY2024.

Diminishment of network perimeter

- Rapid adoption of cloud technologies
- Hybrid remote-work environments
- Increase in mobile access to enterprise applications

M-22-09 Zero Trust Strategic Goals aligned with the 5 Pillars of the CISA Zero Trust Maturity Model

Identity

- Access to enterprise resources managed by a centralized identity access and management system
- Phishing-resistant MFA enforced at the application layer

Device

- Complete and accurate device inventory
- Device health and compliance is ensured prior to enabling authorization
- ► Installation of endpoint detection and response (EDR) tools and established information sharing capabilities

Federal timeline for ZTA implementation

5/12/21 Release of EO 14028

7/11/21 Initial ZTA implementation



plan must be submitted to CISA



Updated ZTA implementation plan for FY22-FY24 and estimated ZTA budget for FY24 must be submitted to OMB and CISA

1/26/22

OMB Memo M-22-09 released



1/26/23

- Public-facing agency systems that support Multifactor Authentication (MFA) must give users the option of using phishing-resistant MFA.
- 1 FISMA Moderate System must be configured for full-featured use over the internet.

9/30/24

All other M-22-09 goals must be met



Network/environment

- Strategically segmented networks with monitoring to identify behavioral anomalies
- Encryption of all Domain Name System requests, HTTP traffic and emails in transit

Application workload

- Applications treated as internet-connected
- Applications routinely subjected to rigorous testing
- Repeatable, immutable workload deployment

Data

- ▶ Data identified, inventoried, classified, labeled and protected
- ► Enterprise-wide logging and information sharing

The EY ZTA Approach expands upon the CISA Zero Trust Maturity Model to provide a robust understanding of your ZTA current state and to help you plan to meet M-22-09 goals.

Integrates with NIST regulatory requirements

Integrates with multiple regulatory requirements and frameworks, including NIST 800-53 and NIST CSF



Maps to the DHS CISA Zero Trust Maturity Model

Maps to the CISA ZTA Maturity Model utilizing the 5 CISA Zero Trust Pillars and capabilities as a baseline

Repeatable process that combines industry-leading methodologies with the CISA Zero Trust Maturity Model to understand the current state and quantify ZTA investments to make informed decisions



Evaluation of additional factors (capability, maturity, adoption) while adjusting to adopt a 5-scale rating model to match standard maturity models

Capability: What can the service do?

Maturity: Is the service operating **effectively**?

Adoption: Is the service being utilized across the enterprise?

EY Zero Trust Services

We offer the full scope of Zero Trust services to support your transformation, including assessment, design, implementation and management.

Assessment

- ► ZTA assessments
- Cyber program assessment
- System assessments
- Penetration testing
- Cloud-readiness assessment
- Software security assessment

Identity

- Identity and access management
- Privileged access management
- ▶ MFA
- Context-aware and conditional access
- Zero Trust policy engine deployment
- User behavior analytics

Device

- Device and asset management
- ► Device trust and compliance
- ► High-value asset identification
- EDR tool deployment and configuration

Networking/environment

- Software-defined networking
- Micro-/macro-segmentation design and deployment
- Network visibility and analytics
- Network management
- SOC services, security monitoring

Application workload

DevSecOps

EY Zero Trust key outcomes

Understanding of ZTA current state

---- Maturity

- Capability

Application Workload

- ► Software supply chain
- ► Granular access control
- Service mesh
- Authentication/authorization models

- Data inventory, classification and identification of critical data
- Broad data loss prevention

ZTA prioritized project list

ZTA roadmap and implementation plan

- Automated data classification and discovery
- Security orchestration and automation

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ev.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ev.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US

2203-3997224 | ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific

ey.com

Data