SUCCESS STORY

EASY DYNAMICS℠

Our implementation strategy advances zero trust as a mission enabler

Easy Dynamics successfully facilitated an agency's transition to a governed zero trust architecture without disrupting its mission-critical work.

Background

OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, mandated that federal agencies align with stringent cybersecurity standards by the end of FY 2024, emphasizing the strategic necessity of transitioning to a resilient zero trust architecture. It directed agencies to advance security measures that reduce the risk of successful cyberattacks against federal digital infrastructure, with requirements organized across the five pillars of zero trust: Identity, Devices, Networks, Applications, and Data.

In order to comply with M-22-09, a federal client first needed a comprehensive review of its IT infrastructure to understand where deficiencies existed, along with a detailed plan for closing the gaps and bringing the agency into timely compliance.

The Challenges

During Year 1 of the contract, our team conducted a benchmark analysis of the agency's infrastructure, policies, and procedures across all locations for each of the zero trust pillars, resulting in a maturity score delivered to the OCIO. Our assessment revealed several challenges that needed to be addressed:

Environmental Complexity

The enterprise environment is geographically distributed and operationally complex, spanning four primary locations that each maintain its own network infrastructure and on-premises data center. Local networks are also logically segmented across each site, using a dual-domain architecture that is categorized by workload profile and access requirements.

Inconsistent Security

Reliance on a traditional perimeter-based security model meant the agency's security and IAM capabilities were implemented unevenly across the enterprise. Identity and access decisions were largely static and policy-driven rather than dynamic and context-aware, leaving gaps in security enforcement across environments.

Underutilized Capabilities

Although the agency's HQ had provisioned advanced tools such as CrowdStrike, Zscaler, CyberArk, and SolarWinds, they were distributed without much guidance. The lack of a cohesive integration strategy or local expertise meant these critical capabilities were either misconfigured or left underutilized.

Our Solution

Easy Dynamics introduced a structured, agile-based change management approach designed to modernize security capabilities without disrupting their business operations. We broke zero trust improvements into discrete, value-driven work packages, assessing each for operational risk and mission impact. After setting up a zero trust working group consisting of government and contractor staff, we prioritized “quick wins” that delivered

immediate security value, sequenced higher-risk changes to align with operational readiness, and introduced agile planning disciplines to track sprints and dependencies. We also supported workforce transformation by assisting with hiring and onboarding personnel with specialized zero trust and security expertise.

The Measurable Results

Our team successfully facilitated the agency's transition from an unassessed, fragmented security posture to a well-governed zero trust ecosystem. Our approach advanced zero trust as a mission enabler rather than a disruptor, integrating a risk-based maturity framework that ensured operational continuity for mission-critical systems.

Year 1 Milestones:

- Formalized a technical baseline across all five zero trust pillars, identifying gaps between current-state and M-22-09 requirements
- Conducted a gap analysis of existing, high-value zero trust capabilities available within the enterprise technology stack to identify and configure dormant functionalities and maximize ROI on existing infrastructure
- Operationalized underutilized zero trust artifacts, including micro-segmentation and enhanced telemetry, while ensuring zero downtime for critical operational environments
- Developed a multi-year phased implementation plan to achieve M-22-09 compliance, including phishing-resistant MFA, internal traffic encryption, and identity-based perimeters

Policy Alignment:

- Prioritized the move toward cloud-based infrastructure and enterprise-wide identity management to advance the agency's M-22-09 compliance
- Utilized CISA's Zero Trust Maturity Model 2.0 to ensure cross-pillar visibility and automated orchestration
- Focused on the "least privilege" zero trust principle to mitigate lateral movement in compliance with NIST SP 800-207

CONTACT US

Greg Gordon
Chief Delivery Officer
ggordon@easydynamics.com

JJ Harkema
VP Solutions & Partnerships
jharkema@easydynamics.com

FEDERAL EXPERIENCE

- Department of Agriculture
- Department of Homeland Security
- Defense Information Systems Agency
- Defense Logistics Agency
- Naval Special Warfare Command
- Federal Law Enforcement Training Center
- National Institute of Standards and Technology
- Cybersecurity and Infrastructure Security Agency
- Internal Revenue Service
- General Services Administration
- Department of the Treasury
- Health & Human Services
- Social Security Administration
- Department of Education

CORE CYBERSECURITY CAPABILITIES

- Enterprise ICAM
- Cloud Modernization
- Automation
- Zero Trust
- Risk Management