SUCCESS STORY

EASY DYNAMICS℠

Closing a critical attack vector through phishing-resistant MFA enforcement

Our successful approach encompassed 1.3K accounts and eliminated one of the most exploited attack vectors in the federal threat landscape.

Background

In December 2024, Easy Dynamics completed a comprehensive ICAM discovery assessment for a federal client that revealed critical gaps in its enforcement of phishing-resistant MFA on Entra ID – a configuration that represented a significant attack surface comprising key business functions like email, instant messaging, and collaboration, as well as critical systems hosted in Azure.

The Challenges

At the outset, the agency faced several compounding authentication security challenges that required immediate remediation, including:

Vulnerable High-Risk Identities

Privileged cloud-only accounts lacked phishing-resistant MFA protection, leaving them vulnerable to adversary-in-the-middle attacks and credential phishing campaigns.

Potential Exploitation Paths

Non-phishing-resistant authentication methods remained active and accessible within government and commercial Entra ID tenants, providing potential exploitation paths.

Federal Non-Compliance

The agency's ICAM posture was out of compliance with several federal requirements, including of EO 14028, OMB M-22-09, and the Credential Management pillar of CISA's Zero Trust Maturity Model. It also represented a significant misalignment of CISA's Binding Operational Directive 25-01, mandating compliance with CISA's SCuBA baseline.

OCM Complexity

Ensuring operational continuity for 1,300 accounts during authentication method transitions demanded a structured, phased approach with robust communication and support.

Our Approach

Easy Dynamics delivered a fully phishing-resistant identity posture across all 1,300 accounts, successfully eliminating agency-wide credential-based attack paths. We began by inventorying every account and the authentication methods in use across privileged and non-privileged populations, then designed Conditional Access baseline policies enforcing phishing-resistant MFA tailored to each population: Certificated-Based Authentication (CBA)/PIV for enterprise users; CBA using a separate privileged certificate and physical authenticator for privileged cloud-only accounts; and FIDO2 security keys paired with physical security measures for emergency access accounts. Coordinating closely with the agency's service desk to preserve uninterrupted access, we then enforced those policies, disabling all non-phishing-resistant credentials without an authorized exemption and confirming 100 percent coverage through a full attestation sweep. Our team then codified the new standards in ICAM governance documentation.

The Outcome

Credential Attack Surface Eliminated

All non-phishing-resistant authentication methods were fully disabled across both Entra ID tenants, closing the

primary credential exploitation vector.

Zero Trust Maturity Advancement

The agency's ZTMM Credential Management pillar advanced to optimal maturity posture, satisfying OMB M-22-09 phishing-resistant authentication requirements, CISA zero trust benchmark criteria, and compliance with the authentication requirements of BOD 25-01.

Enterprise-Wide Compliance Achieved

All user accounts achieved phishing-resistant MFA compliance within the twelve-month enforcement window.

Privileged Identity Risk Reduced

Cloud-only privileged accounts were migrated from username/password authentication to phishing-resistant credential methods.

Operational Continuity Maintained

Through phased rollout and proactive OCM, the agency's workforce transitioned to phishing-resistant authentication with zero major operational disruptions reported during enforcement.

Foundation for Future ICAM Maturation

The enforcement program established the credential management baseline for downstream ICAM initiatives, including passwordless authentication roadmap development, FIDO2 expansion, and Entra ID Conditional Access policy maturation.

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