Forcepoint

TIMELINE

The Federal Quest for Zero Trust

MAY 2018

ACT-IAC ZERO TRUST

Federal CIO Council Services, Strategy, and Infrastructure Committee asked ACT-IAC to evaluate the technical maturity, availability for procurement, and important issues related to potential federal agency adoption of zero trust cybersecurity.

AUG 2020

NIST SP 800-207

Defines a zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

FEB 2021

NSA EMBRACING A ZERO TRUST SECURITY MODEL

Provides NSA's customers with a foundational understanding of Zero Trust, discusses its benefits along with potential challenges, and makes recommendations for implementing Zero Trust within their networks.

APR 2021

DOD ZERO TRUST REFERENCE ARCHITECTURE

Instructs DOD to prioritize Zero trust to create "a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat."

MAY 2021

EXECUTIVE ORDER 14028

Among other policy mandates, the EO embraces zero trust as the desired model for security and tasks agencies with modernizing cybersecurity programs, services, and capabilities to work with cloud-computing environments and follow zero trust architectures (ZTA).

JUN 2021

CISA ZERO TRUST MATURITY MODEL

Assists agencies in the development of their Zero Trust strategies and implementation plans, and present ways CISA services can support zero trust solutions across agencies. CISA's zero trust model describes five pillars of Zero Trust with three themes that cut across each area. CISA is expected to release the 2.0 version of the maturity model soon.

JAN 2022

OMB M-22-09

Requires agencies to have a plan now to achieve specific zero trust security goals by the end of Fiscal Year (FY) 2024, leveraging the zero trust maturity model developed by CISA.

JUL 2022

NIST CYBERSECURITY PRACTICE GUIDES

The National Cybersecurity Center of Excellence (NCCoE) aiming "to remove the shroud of complexity around designing for zero trust with "how to" guides and example approaches to implementing a zero trust architecture for several common business cases."

EXP 2022

DOD ZERO TRUST STRATEGY

The DoD initial strategy for Zero Trust focuses on interoperability and specifies requirements without being overly prescriptive to enable each component in DoD to implement ZT capabilities in the way that is most appropriate for its particular needs, while still maintaining compliance with issued guidance — namely, the Zero Trust Reference Architecture.

2024 Federal Zero Trust Goals

1. Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.
2. Agencies must use strong MFA throughout their enterprise.
3. When authorizing users to access resources, agencies must consider **at least one device** level signal alongside identity information about the authenticated user.

Download the latest report to learn about the progress and challenges agencies face as they move toward Zero Trust Security.

Download Report →

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

Forcepoint

Forcepoint.com