CLOUDFLARE
AREA 1 SECURITY

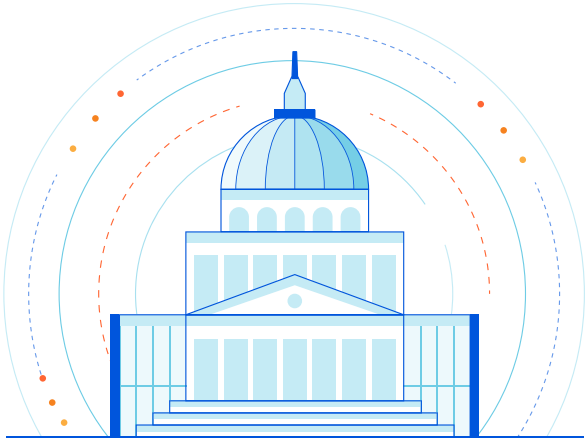
SOLUTION BRIEF

Cloudflare Area 1 Security for Continuous Diagnostics and Mitigation

Strengthen cybersecurity programs with advanced email security

Since its launch in 2013, the Continuous Diagnostics and Mitigation (CDM) Program has been instrumental in helping federal departments and agencies improve their cybersecurity strategies.

Led by the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security (DHS), the CDM's stated goals are to reduce threat surface area, increase visibility into cybersecurity posture, improve response capabilities, and streamline reporting. The CDM program also aligns with a May 2021 Executive Order on "Improving the Nation's Cybersecurity" from U.S. President Joe Biden, highlighting the importance of improving detection, investigation, and responses to cybersecurity incidents.



The CDM Program is divided into the following four phases:

Phase 1: Access Management

What is on the network?

Phase 2: Identity and Access Management

Who is on the network?

Phase 3: Network Security Management

What is happening on the network? How is the network protected?

Phase 4: Data Protection Management

How is data protected?

Cloudflare Area 1 Security supports agencies in fortifying their security programs to help achieve their CDM goals and requirements. The following table provides more details on each functional area of the CDM Program, and how Area 1 email security can help agencies with their CDM initiatives.

CDM phases	Cloudflare Area 1 Security mapping
Phase 1: Manage assets Hardware asset management (HWAM) Software asset management (SWAM) Configuration settings management (CSM) Vulnerability management (VUL)	**N/A** **(Phase 1 is best addressed by solutions providing asset visibility and management for organizations)**
Phase 2: Manage Accounts for People and Services Manage trust in people granted access (TRUST) Manage credentials and authentication (CRED) Manage privileges (PRIV) Manage security-related behavior and training (BEHAVE)	• Stops credential harvesting and account takeover (ATO) attacks which are related to breach of trust; Area 1's Enterprise and PhishGuard customers are notified of fraud attempts • Uses six methodologies and technologies for fraud prevention, including close inspection of behavioral indicators (message sentiment analysis, conversational context analysis, and others) extending to trusted partners and suppliers
Phase 3: Manage Events Boundary protection (BOUND) Prepare for incidents and contingencies Detect suspicious events and patterns Respond to incidents and contingencies	• Preemptively stops phishing attacks before they reach inboxes, the equivalent of the modern enterprise boundary • Stops hard-to-detect attacks like drawn out supply chain-based business email compromise (BEC) for supply chain risk management • Provides automated detections and triage with multi-level forensics for easy incident investigations • Built-in response options like Message Retraction improve response time to incidents
Phase 4 - Data Protection Data discovery and classification (DISC) Data protection (PROT) Data loss prevention (DLP) Breach mitigation (MIT) Information rights management (IRM)	• Protects against loss of data and funds from ransomware and BEC attacks • Protects against insider threats; PhishGuard customers also receive customized notification and responses • Partnership with Virtru combines end-to-end encryption and DLP with advanced cloud-native email security capabilities

How Cloudflare Area 1 Security can help

Area 1's preemptive and comprehensive email security service helps organizations of all sizes improve their security posture and meet requirements of federal security programs such as CDM, through secure cloud services.

With phishing as the root cause of most cyber breaches, a robust security program requires advanced email security with end-to-end detection-to-response capabilities like those provided by Area 1, which is part of the Cloudflare Zero Trust platform.

Contact publicsector@cloudflare.com to learn more about Cloudflare Zero Trust cybersecurity for government agencies, or click here for more about Area 1.