AREA 1


Microsoft Partner

# 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 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: Identify what is on the network**
**Phase 2: Identify who is on the network**
**Phase 3: Identify what is happening on the network**
**Phase 4: Determine how data is protected**

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 phase of the CDM Program, and how Area 1 can help agencies in with their CDM initiatives.

| CDM PHASES | AREA 1 SECURITY MAPPING |
|---|---|
| **PHASE 1: MANAGE ASSETS**<br>Hardware asset management (HWAM)<br>Software asset management (SWAM)<br>Configuration settings management (CSM<br>Vulnerability management (VUL) | N/A<br>(Phase 1 is best addressed by solutions providing asset visibility and management for organizations) |
| **PHASE 2: MANAGE ACCOUNTS FOR PEOPLE AND SERVICES**<br>Manage trust in people granted access (TRUST)<br>Manage credentials and authentication (CRED)<br>Manage privileges (PRIV)<br>Manage security-related behavior and training (BEHAVE) | • Stops credential harvesting and account takeover (ATO) attacks which are related to breach of trust; Area 1 Horizon and PhishGuard customers are notified of fraud attempts<br>• Uses six methodologies and technologies for Active Fraud Prevention, including close inspection of behavioral indicators (message sentiment analysis, conversational context analysis, etc.) extending to trusted partners and suppliers |
| **PHASE 3: MANAGE EVENTS**<br>Boundary protection (BOUND)<br>Prepare for incidents and contingencies<br>Detect suspicious events and patterns<br>Respond to incidents and contingencies | • Preemptively stops phishing attacks before they reach inboxes, the equivalent of the modern enterprise boundary<br>• Stops hard-to-detect attacks like drawn out supply chain-based Business Email Compromise (BEC) for supply chain risk management<br>• Autonomous Phish SOC provides automated detections and triage with multi-level forensics for easy incident investigations<br>• Built-in response options like Message Retraction improve response time to incidents |
| **PHASE 4 - DATA PROTECTION**<br>Data discovery and classification (DISC)<br>Data protection (PROT)<br>Data loss prevention (DLP)<br>Breach mitigation (MIT)<br>Information rights management (IRM) | • Protects against loss of data and funds from ransomware and BEC attacks<br>• Protects against insider threats; PhishGuard customers also receive customized notification and responses<br>• Partnership with Virtru combines end-to-end encryption and DLP with advanced cloud email security capabilities |

AREA 1

*How Area 1 Security Can Help*

Area 1's preemptive and comprehensive security solution helps organizations of all sizes improve security posture and meet requirements of federal security programs such as CDM, through secure cloud services in alignment with U.S. executive orders.

With email 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 of Area 1.

*To learn how Area 1 Security can help meet CDM guidelines and strengthen your security defenses, visit https://www.area1security.com/about/contact-us/.*

# About Area 1 Security

Area 1 Security is the only company that preemptively stops Business Email Compromise, malware, ransomware and targeted phishing attacks. By focusing on the earliest stages of an attack, Area 1 stops phish — the root cause of 95 percent of breaches — 24 days (on average) before they launch. Area 1 also offers the cybersecurity industry's first and only performance-based pricing model, Pay-per-Phish.

Area 1 is trusted by *Fortune* 500 enterprises across financial services, healthcare, critical infrastructure, and other industries, to preempt targeted phishing attacks, improve their cybersecurity posture, and change outcomes.

Area 1 is cloud-native, a Certified Microsoft Partner, and Google Cloud Technology Partner of the Year for Security. To learn more, visit www.area1security.com, follow us on LinkedIn, or subscribe to the Phish of the Week newsletter.