

# ACHIEVING MISSION SUCCESS WITH CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)

Building Cyber Operational Agility into Federal IT

## CDM – AN INTRODUCTION

As the Continuous Diagnostics and Mitigation (CDM) program matures, it requires a new way of thinking. While agencies will continue to buy tools to fill gaps in their defenses, they need to start thinking about how those tools fit into their larger cybersecurity strategy.

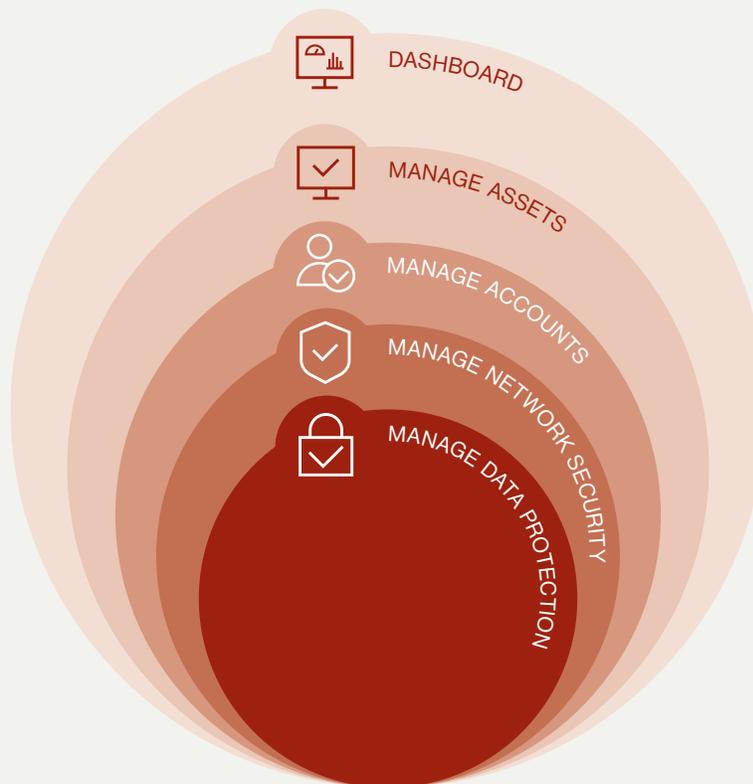
The CDM program has shifted from one previously organized by phases to one that is now organized by capability areas defined by asset management, identity and access management, network security management, and data protection management as referenced in Figure 1.

The initial task orders under the program were tool-oriented, with a focus on automating the ability to identify, profile and scan assets on the network and improve visibility into credentialed and privileged users. Task orders related to these initial phases were issued against the (now retired) CDM Tools/Continuous Monitoring as a Service (CMaaS) blanket purchase agreements, and typically ran two or three years.

CDM efforts shifted gears with the current Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) program. DEFEND ushers in a move away from “phases” and toward “capability areas” that focus on more advanced capabilities, including incident response, mobile security, cloud security, network access controls and data protection.

DEFEND has also laid the groundwork for a shift from a “compliance-focused” security to one of true “operational security improvement,” providing agencies with the ability to be creative and to implement innovative solutions that can have a meaningful impact. CDM requirements also dovetail nicely with the White House’s current IT modernization efforts.

Figure 1. CDM Capability Areas



# CROWDSTRIKE ENABLES CDM

CrowdStrike® is uniquely positioned to help deliver on the main goal of CDM: **Cyber Operational Excellence**. CrowdStrike natively supports and enables federal agencies and organizations by intelligently bridging the gap between the Federal Cloud First/Cloud Smart initiatives and the modernization mandate of CDM DEFEND that encourages the adoption of cloud-based cybersecurity technologies and protection of cloud-based assets. Agencies already understand and have realized the agility and cost benefits associated with the software-as-a-service (SaaS) model provided in the form of CRM, HR and other business-critical solutions. CrowdStrike has extended those benefits to cybersecurity and leads the industry with its cloud-native architecture. CrowdStrike solutions drive down the cost and complexity associated with legacy security architectures that have proven unable to meet the latest challenges in information security.

The CrowdStrike Falcon® platform provides federal agencies with the unique ability to upgrade their current cyber operations capabilities to detect and prevent never-before-seen attacks while they are still in progress — protecting them against threats their conventional defenses can't even see.

CrowdStrike industry leadership has helped define an entirely new science for detecting adversary activity before it is too late with the CrowdStrike Security Cloud, the world's largest unified, threat-centric data fabric, powering the next generation of protection and elite threat hunting to stop breaches. Security Cloud correlates trillions of security events per day with indicators of attack, the industry's leading threat intelligence and enterprise telemetry from across customer endpoints, workloads, identities, DevOps, IT assets and configurations. Using cloud-scale AI and machine learning, the CrowdStrike Security Cloud also creates actionable data, identifies shifts in adversarial tactics, and maps tradecraft in the patented Threat Graph to automatically prevent threats in real time across CrowdStrike's global customer base.

The CrowdStrike Falcon Platform is both FedRAMP Authorized and listed on the CDM Approved Products List (APL).

## A COMPREHENSIVE PLATFORM FOR DEFENSE IN BREADTH



VIA A SINGLE LIGHT-WEIGHT, CLOUD-NATIVE AGENT

Figure 2. The CrowdStrike Falcon platform aligns with the Mitre Att&ck™ framework and addresses many areas of each CDM phase.



## CDM MODERNIZATION

The MGT Act, along with the American Technology Council's "Report to the President on Federal IT Modernization," calls on agencies to use new and emerging technologies, such as cloud computing, to replace older systems that impose an increased security risk.

Most agency security architectures were designed prior to the use of software-as-a-service (SaaS) and other "as-a-service" offerings critical to delivering cyber capabilities with the speed and agility required in the twenty-first century.

As federal agencies meet CDM goals, they can use the program as a springboard to improve their overall cyber capabilities. For many agencies, this will involve an in-depth defense approach, where they build security architectures into a cohesive system structured around cyber visibility.

Because today's federal agencies closely resemble and are expected to deliver services similar to other modern work environments, the convergence of CDM DEFEND, along with larger U.S. Government IT modernization efforts, provides a real opportunity for improving agencies' abilities to go far beyond scanning baselines and asset baselines in favor of modern, integrated cyber defense platforms. These new platforms can empower robust cyber operations capabilities, including positively identifying meaningful and relevant indicators, operationalizing analysis of threat intelligence, and orchestrating responses.

Most security architectures, including early stage CDM technologies, are myopically focused on identifying assets and vulnerabilities in the hopes of stopping malware. However, the problem is no longer just about malware and vulnerabilities — it is about the adversaries themselves. This new breed of adversary is extremely skilled, often well-funded and utterly relentless in outsmarting and bypassing malware-based defenses. The modern cyber resilience challenge is about identifying these sophisticated adversaries — detecting their actions at the earliest possible stage of an attack, and actively preventing their attacks from becoming damaging security breaches — precisely the ultimate goal of CDM.



# MAPPING CROWDSTRIKE AND CDM

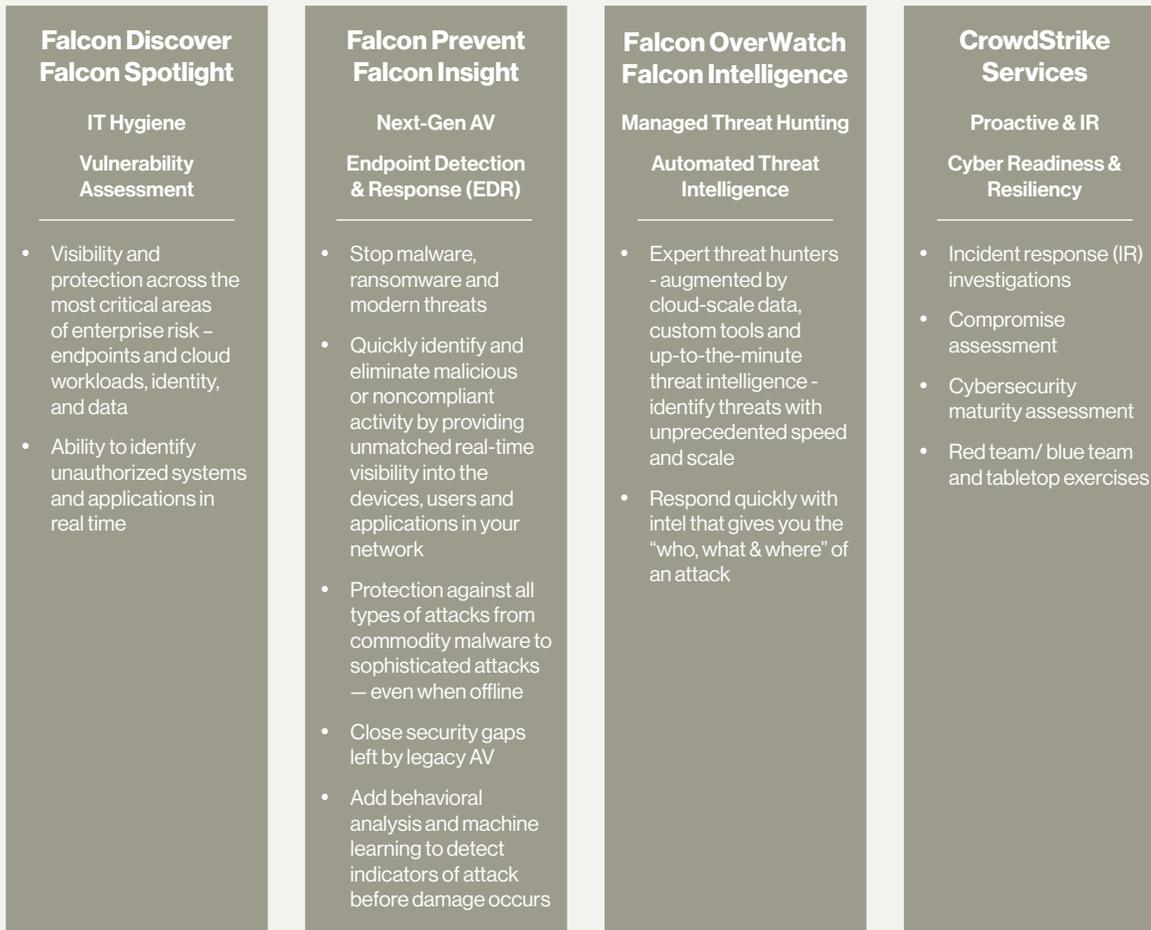
The flexibility of the innovative CrowdStrike Falcon platform offers federal agencies a host of capabilities that map directly to requirements spanning multiple phases of the CDM program. CrowdStrike's extensible technology and unparalleled fidelity of captured data equally enable the established compliance-based security mandates of CDM, as well as deliver on the ultimate goal of superior cyber operational agility. Figure 3 provides a general mapping of where and how the CrowdStrike platform enables CDM:

## MAPPING CROWDSTRIKE AND CDM

Manage Assets (Phase 1):  
What's on the network?

Manage Network Security (Phase 3):  
What is happening on the network

CDM DEFEND (Task 5):  
Surge Response



**Integrated Platform, Cloud-Native Architecture, Powered by Intelligence, Delivered Via One Lightweight Agent**

Figure 3. This diagram shows how CrowdStrike capabilities map to the CDM program.



**Falcon Discover: IT Hygiene to Prepare & Prevent**

Falcon Discover allows you to quickly identify and eliminate malicious or noncompliant activity by providing unmatched real-time visibility into the devices, users and applications in your network.

**Falcon Spotlight: Scanless Vulnerability Management**

Falcon Spotlight provides real-time visibility across your enterprise — giving you relevant and timely information you need to reduce your exposure to attacks with zero impact on your endpoints

**Falcon Prevent: Cloud-native Next-Generation Antivirus (NGAV)**

Falcon Prevent offers the ideal AV replacement solution by combining the most effective prevention technologies with full attack visibility and simplicity — you'll be up and ready immediately.

**Falcon Insight: Endpoint Detection and Response (EDR)**

Falcon Insight delivers continuous, comprehensive endpoint visibility that spans detection, response and forensics to ensure nothing is missed and potential breaches are stopped

**Falcon OverWatch: Managed Threat Hunting**

Falcon OverWatch™ is a human threat detection engine that operates as an extension of your team, hunting relentlessly to see and stop the most sophisticated hidden threats

**Falcon Intelligence: Automated Threat Intelligence**

Supercharge your SOC and Incident Response teams with built-in adversary intelligence and get ahead of the attackers next move.

**CROWDSTRIKE SERVICES**

CrowdStrike Services helps organizations train for, react to and remediate a breach quickly and effectively — getting you back to business faster.



# NAVIGATING CDM

Understanding, let alone navigating, the intricacies of a program as wide-reaching as CDM can be daunting. CrowdStrike wants to partner with you to ensure your organization's success with the CDM program. Aside from meeting many of the program's technical requirements, the inclusion of the Falcon platform on the CDM Approved Products List (APL) and CrowdStrike's commitment to helping modernize your agency's cyber capabilities can ensure a successful implementation. In addition, CrowdStrike can assist with navigating the program itself, and the processes involved with acquiring and leveraging the capabilities associated with CDM.

## HOW TO REQUEST CROWDSTRIKE'S HELP

The following graphic provides a glimpse into the Request for Service (RFS) process introduced with CDM DEFEND. This process improves CDM effectiveness for agencies by capitalizing on the successes of the early CDM phases, while simultaneously leveraging lessons learned to eliminate common obstacles to adoption.

**For assistance, please contact CrowdStrike Federal Sales directly at email: [CDM@CrowdStrike.com](mailto:CDM@CrowdStrike.com)**

### CDM DEFEND: REQUEST FOR SERVICE PROCESS

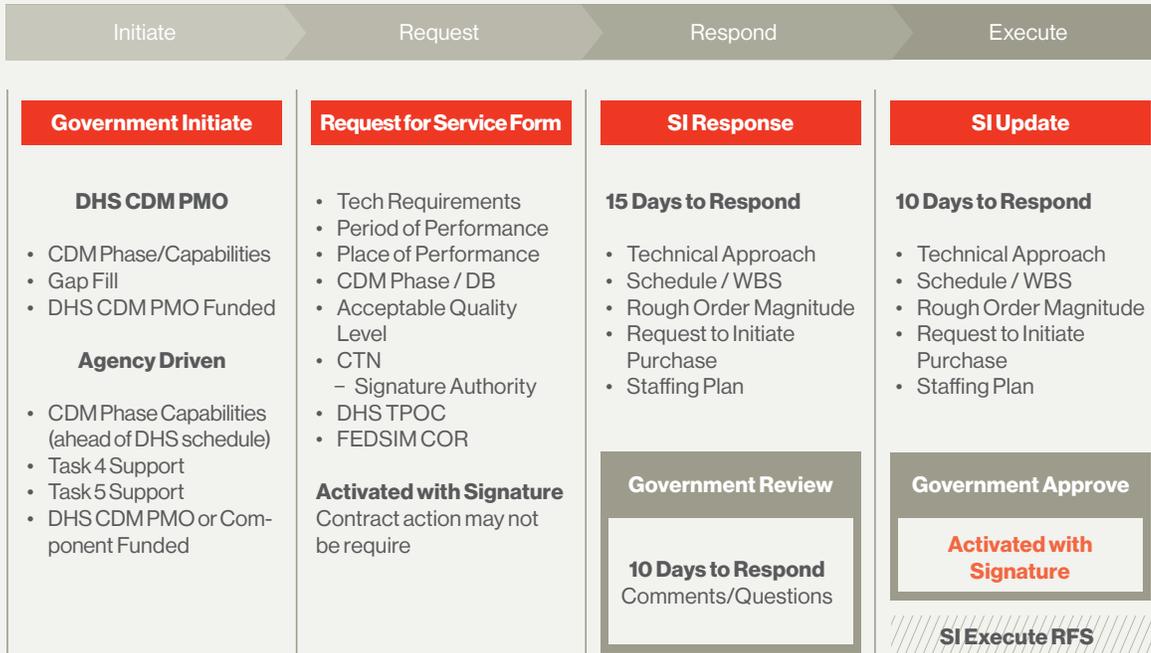


Figure 4. This diagram shows the phases of the CDM DEFEND RFS process.



## THE BENEFITS OF USING THE CDM RFS PROCESS:

- Accelerates the acquisition timeline to ensure streamlined procurement
- Controls CDM architectural strategy: defines and retains the desired standards for the agency
- Reduces risk through demonstrated alignment to guidance (OMB 19-02)
- Prioritizes the right cyber investments to align with your agency's cyberstrategy
- Expands and augments access to funding to deploy critical capabilities to the enterprise

## WAYS TO LEVERAGE THE CDM PROCESS:

- Map planned cyber investments to CDM Capability Areas: CDM is an enabler
  - Review the full scope of planned and prioritized cyber investments/enhancements
  - Map those against CDM requirements — understand where the program can enable agency strategy
  - Identify connectivity to early phase capabilities and requirements to drive prioritization of prospective RFS
- Develop a baseline RFS: define agency standards and detail requirements
  - Draft the RFS with a focus on tying it to initial CDM capabilities
  - Justify prioritization of that technical capability in your environment
  - Target near-term, high-value CDM functional capability (visibility, what's not working, cloud, etc.)
- Engage CDM PMO: gain insight into their prioritization
  - Be an active participant in the dialog and a voice for your agency's agenda
  - Understand its guidance for getting what you need from your integrator
  - Identify Intersection with external policy mandates
    - HVA Program
    - MEGABYTE Act
    - MGT Act/ modernization initiatives
- Contribute funding: funding your own RFS for cyber investments through DEFEND has many benefits
  - Accelerated acquisition with reduced paperwork requirements
  - Ability to expand/augment funding to take pilots to enterprise deployments
  - Allows you to control your standards and architectural strategy through the program as an active participant
  - Ensures alignment to OMB 19-02/03



## CDM BACKGROUND

In 2012, the Office of Management and Budget (OMB) identified continuous monitoring of federal IT networks as one of 14 Cross-Agency Priority Goals, established in accordance with the Government Performance and Results Modernization Act (GPRMA).

Subsequently, the Department of Homeland Security (DHS) established the CDM program to “support government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity.”

The CDM program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

The goals and objectives of the program are:

- Reduce agency threat surface
- Streamline Federal Information Security Modernization Act (FISMA) Reporting
- Increase visibility into the federal cybersecurity posture
- Improve federal cybersecurity response capabilities

In August 2013, the DHS, in partnership with the General Services Administration (GSA), established governmentwide Blanket Purchase Agreements (BPAs) known as the CDM Tools/Continuous Monitoring as a Service (CMaaS). The CDM Tools/CMaaS BPAs expired in August 2018 and were replaced with a new dual-pronged acquisition strategy: **CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND)**.

## ABOUT CROWDSTRIKE

**CrowdStrike** Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world’s most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:

<https://www.crowdstrike.com/>

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

Start a free trial today:

<https://www.crowdstrike.com/free-trial-guide/>

© 2022 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.



Learn more: [www.crowdstrike.com/security-solutions/government-public-sector/](https://www.crowdstrike.com/security-solutions/government-public-sector/)

CrowdStrike Products are FedRAMP Authorized



# CROWDSTRIKE FALCON: A RADICAL NEW APPROACH PROVEN TO STOP BREACHES

CLOUD-DELIVERED PROTECTION ACROSS ENDPOINTS, CLOUD WORKLOADS, IDENTITY AND DATA



A single agent solution to stop breaches, ransomware, and cyber attacks—powered by world-class security expertise and deep industry experience. Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon Platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

## WHY CROWDSTRIKE FALCON?

### CLOUD NATIVE

Eliminates complexity and simplifies deployment to drive down operational costs

### AI Powered

Harnesses the power of big data and artificial intelligence to empower your team with instant visibility

### Single Agent

Delivers everything you need to stop breaches — providing maximum effectiveness on day one



**CROWDSTRIKE CORPORATE HEADQUARTERS**  
**150 MATHILDA PLACE, SUITE 300 SUNNYVALE, CA 94068**

info@crowdstrike.com | publicsector@crowdstrike.com | crowdstrike.com

**Experienced a breach?** Contact us at (855) 276-9347

or services@crowdstrike.com

CrowdStrike Products are FedRAMP Authorized