

The Okta logo is rendered in a bold, lowercase, blue sans-serif font. The letters are thick and rounded, with a consistent weight throughout. The 'o' is a simple circle, and the 'k' has a slightly curved stem. The 't' is a simple vertical bar with a horizontal crossbar, and the 'a' is a simple rounded shape. The logo is positioned in the lower-left quadrant of the page, set against a white background with large blue curved shapes on the left and bottom edges.

okta

Modernizing
Cyber Defense:
Embracing CDM

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

The Department of Homeland Security's (DHS) Continuous Diagnostic and Mitigation (CDM) program gives Federal agencies a first-of-its-kind opportunity to get in front of cyber threats, delivering new insights into what and who is on the network for 23 Chief Financial Officer (CFO) Act agencies, plus as-a-service to more than 44 non-CFO Act agencies.

In a recent Congressional hearing, CDM program manager Kevin Cox testified the program is making a significant impact in providing agencies with improved network visibility and control. With greater knowledge of what's connected, the National Protection and Programs Directorate (NPPD) at DHS has more confidence in managing threats, compared to the previous system of agency self-reporting.

"CDM is changing this model, enabling NPPD to immediately view the prevalence of a given software product or vulnerability across the Federal government," Cox said. "The real key for us is to get from a reactive stance to a proactive. We want to get out in front of the threat."



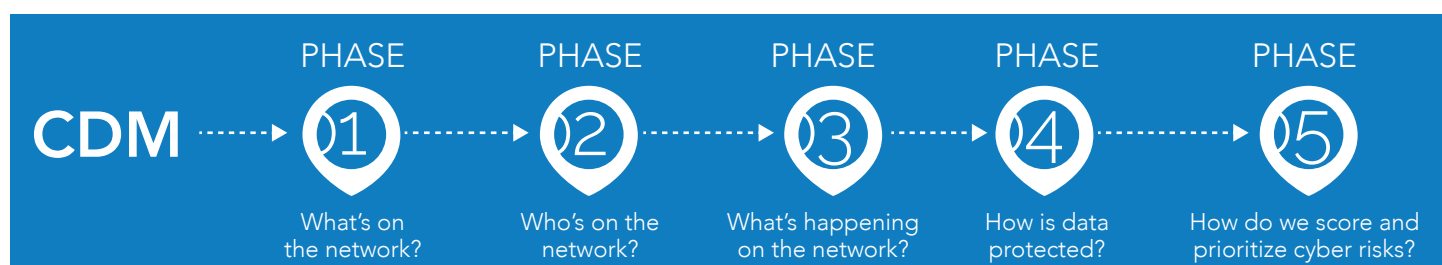
IDENTITY MATTERS

CDM's initial phases focus hard on Identity and Access Management – (IAM). Today, with the preponderance of cloud, mobile, and social networks, there are different types of identities, platforms, and technologies not addressed by traditional identity management measures – creating ever-widening vulnerability gaps due to fractured user authentication and authorization across applications and resources.

Historically, identity and access management focused on managing user accounts; it is often not actually involved in managing identities, let alone multiple types, as is needed in a Cloud First, highly mobile environment. In addition to the multiple types of identities and technologies, IM must also enable the creation of policies and procedures aligned with each agency's unique mission.

Identity management answers the question, "who is on my network?" and must also help address one of the first, core CDM questions, "what is on my network?" on an ongoing basis and support shared services deployment by managing apps via the creation and management of an enterprise app store.

The Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure and the recent Report to the President on Federal IT Modernization emphasize Federal shared services as a critical component to improving security and increasing efficiency. A secure app store, coupled with an IAM solution, enables self-service and automated provisioning within a rules-based environment, and facilitates centralized resource utilization monitoring.



Modern identity and access management, as emphasized in multiple phases of the CDM program, strengthens cyber defenses and enables efficient, scalable, and importantly – secure – IT services delivery.

Okta, a FedRAMP authorized Identity-as-a-Service (IDaaS) provider and two-time leader for the Gartner Magic Quadrant for Access Management is an approved vendor for all three implemented phases of CDM, delivering capabilities for:



Through the CDM program, Okta strengthens and modernizes security while accelerating time to value for new solutions as agencies build modern multi-cloud environments.

CDM PHASE I: VISIBILITY AND VALUE

CDM Phase I gives agencies visibility into what is on their networks.

Phase 1 Target Capabilities

- Hardware Asset Management (HWAM) encourages agencies to find all addressable devices, determine if they are valid, and understand the differences in risk management for the devices
- Software Asset Management (SWAM) calls for agencies to understand what software they access, what the baseline is for usage, and their authorization for the software
- Configuration Settings Management (CSM) employs agencies to understand their baseline settings, policy variance, authorizations, and risk management differences
- Vulnerability Management (VUL) requires agencies to detect, score, and track characteristics of vulnerabilities

Okta’s Always On capability provides real-time software access, usage, and application access denial data based on secure identity management, multi-factor authentication, and single sign-on access control of applications. With these capabilities, Okta’s cloud-focused solutions provide a single source of the truth for the application environment – insights into what users, devices, and software are on the network at all times, whether in the cloud, on-premises, or via mobile devices.

Often deployed in days, Okta can generate built-in and custom reports through an Event API (application programming interface). These reports can supply data to external reporting and SIEM (security information and event management) platforms, including Splunk, ServiceNow, and RSA Archer, reducing deployment risk and expediting time to value.

Center for Medicare and Medicaid Services (CMS) uses the Okta Identity Cloud to monitor for anomalous login behaviors in support of reimbursements to over 1 million health care providers through its Quality Payment Program.

PHASE 2: CREDENTIALING, COLLABORATION, AND CLOUD CLOUD

CDM Phase 2 focuses on who is on the network, giving agencies visibility into who has access, how those users behave on the network, and if users have the correct privileges.

Phase II Target Capabilities

- TRUST certifies that only properly vetted and validated employees get access to systems and credentials
- BEHAVE ensures that individuals receive proper awareness training and exhibit appropriate security-related behavior
- CRED helps agencies with the management of credentials for physical and logical access to guarantee that only authorized people have access to the areas required for their jobs
- PRIV provides insight into the risks associated with various privileges



As the only neutral IDaaS cloud vendor with FedRAMP authorization, Okta provides an essential element of the identity solution mix for CDM Phase 2.

Traditional on-premises identity and discovery tools struggle to provide visibility into cloud applications – leaving agencies with a significant blind spot. Okta logs and audits every event that occurs within the service across all environments, giving detailed information on application usage, login attempts (successful and unsuccessful), active user information, and other activities such as account creation and deletion. This data can be exported to other security tools.

This phase also changes how agencies buy CDM by introducing a two-pronged acquisition strategy. The DEFEND (Dynamic Evolving Federal Enterprise Network Defense) acquisition strategy will use the GSA's Alliant GWAC and Alliant 2 contracts, which will extend task orders to 5-6 years in duration, compared to current 1-2 year duration. The new contracts also will increase the dollar value of awards, providing an opportunity to make larger, longer-term purchases.

Through its integrations with CyberArk and Sailpoint, Okta can fulfill the entire identity solution requirement. Okta specifically helps agencies with credential management (CRED), automation of valid user registration (TRUST), and support of cloud application access certification (PRIV).

The Federal Communications Commission (FCC) turned to Okta Lifecycle Management to help simplify automated provisioning and de-provisioning. These tools are especially important for ensuring employee credentials are consistent with their status during the onboarding and off-boarding processes.

PHASE 3: INCIDENT RESPONSE AND AUTHORIZATION

This phase includes ongoing assessment of the measures taken in previous phases, adding a focus on achieving a real-time view and understanding of what's happening on the network. Phase 3 capabilities enable agencies to introduce automated response to threats and events, and present dashboard results making audits cheaper, quicker, and more accurate. Phase 3 is intended to provide



agencies with continuous monitoring capabilities, reducing their audit dependencies and the frequency of failed audits.

Agency cybersecurity managers will be able to address network activity with a master system record, and then feed agency results into the program-wide dashboard that monitors for threats and compares the progress of different agencies. Key capabilities in this phase include network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities.

Having identified what and who is on agency networks in Phases 1 and 2, Okta, when integrated with other security services, supports the Phase 3 mission of creating and leveraging the master system record to standardize incident reporting and build toward the goal of automated detection and response.

Creating the ecosystem for more automated and systematic responses to threats requires security solutions that are proven to play well with others – in other words, solutions that can integrate and communicate seamlessly within and between agency systems. Okta's successful and proven integrations with leading security partners, such as Palo Alto Networks, Sailpoint, CyberArk, Service Now, Skyhigh Networks, and Cisco Cloudlock (among many others), provide the means to enforce shared access policies.

WHAT'S NEXT FOR CDM

In Phases 1, 2, and 3, agencies are building the "radar" – understanding what's happening inside discrete agency networks, detecting patterns, and locating threats – and taking the first steps toward automated reporting and response. Phase 4, which focuses on how the data is protected, is designed to improve Federal threat response with proactive diagnosis and strategies.

The objective of Phase 4 is to manage security more strategically. CIOs and senior agency leaders will have improved visibility through dashboards that provide a detailed summary and the ability to drill down for actionable detail – improving cyber transparency and accountability. Agency cyber leaders can prioritize risks, to enable timely responses to the most significant problems.

MORE AWARE

Beginning in Federal FY 2019, Phase 5 – Agency Wide Adaptive Risk Enumeration, or AWARE – will be a government-wide cyber risk scoring initiative aimed at measuring how effectively agencies are practicing “cyber hygiene” and reducing their attack surfaces.

The vision of CDM – the cross-agency CDM Dashboard and risk management strategy – requires a foundation of solutions that connect to the device and user endpoints and network gateways, integrated horizontally within agencies and vertically to the level of agency CIOs, agency and department senior leadership, and the Federal CIO.

THE FULL PICTURE

With the right data from both on-premises and cloud environments, Okta’s solutions help agencies gain visibility into what users are doing in any application that houses or touches their data, expanding the possibilities for cyber response. Okta also enables a strong response to

prevent insider threats, as automated de-provisioning of credentials keeps employees from interfering with areas outside of their scope. Okta’s real-time monitoring of both on-premises and cloud software can help trigger security responses when attempts at access raise concerns.


Okta’s identity management capabilities provide a foundational technology for Phase 5 cyber hygiene goals and effectively reduce the attack surface by enabling secure access to applications plus visibility into all interaction with these applications. Cyber leaders can easily evaluate who has access to what, and adjust as needed. The cloud-based architecture provides a highly scalable solution that can accommodate millions of users inside the Federal government and its millions of citizen customers.



LEARN MORE

The CDM program presents a unique opportunity to improve cyber awareness and create a more secure network. Learn more about how to modernize your security infrastructure and Okta’s FEDRAMP-authorized CDM tools: monitoring capabilities to provide visibility, identity solutions to manage access, and visibility tools to enable quick responses.

 www.okta.com

 1-888-722-7871

 info@okta.com

- *Leader, 2018 Gartner Magic Quadrant for Access Management*
- *FedRAMP Authorized Identity-as-a-Service Provider*

okta