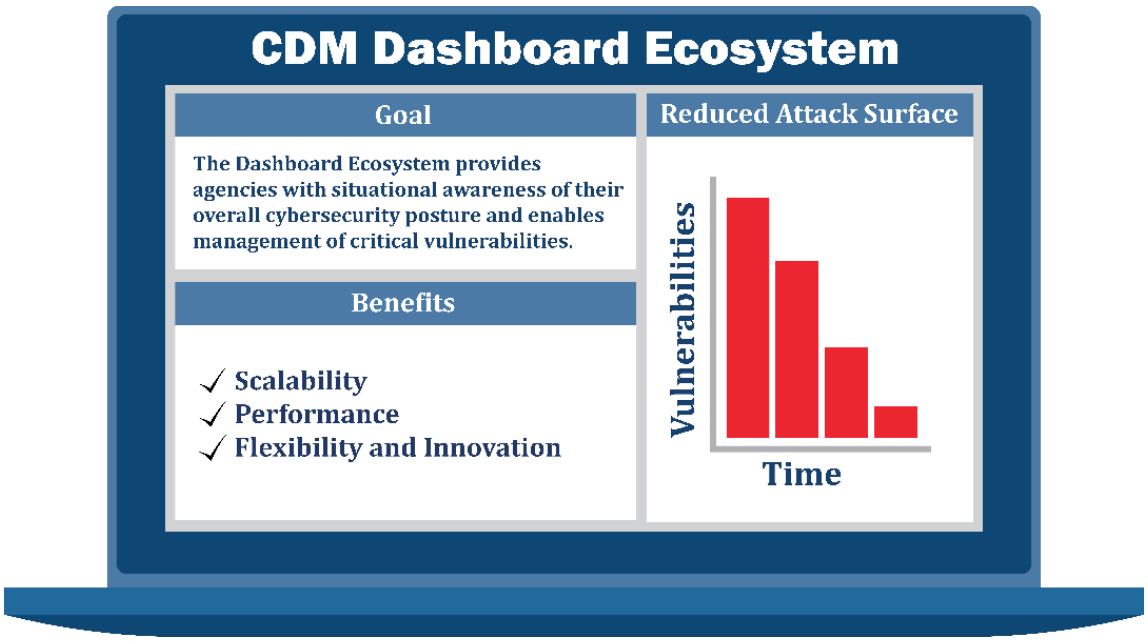
CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM
DASHBOARD ECOSYSTEM

The CDM Program is a dynamic approach to fortifying the cybersecurity of civilian government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies that support them with improving their respective cybersecurity postures.

BACKGROUND

The CDM Dashboard Ecosystem is a collection of complementary tools and services that agencies can use to better understand, prioritize, and mitigate cyber risks. The CDM Agency Dashboards collect and display information gathered from sensors and tools for each participating agency. Each CDM Agency Dashboard feeds summary information to the CDM Federal Dashboard, providing an integrated view of the ".gov" network, ensuring that when a heightened vulnerability or cyberattack occurs on one agency network, federal stakeholders can communicate that threat to all other agencies. The CDM Dashboard Ecosystem provides the situational awareness needed to enable timely remediation of threats and vulnerabilities. It also informs operational and security decisions, which ultimately helps to reduce risk.

The CDM Program has deployed Agency Dashboards to 23 Chief Financial Officers (CFO) Act federal civilian agencies and to many small agencies through the CDM Shared Services Platform. The CDM Dashboard Ecosystem's first release, targeted for Quarter 3 Fiscal Year 2020, will include object-level hardware asset management, configuration settings management, vulnerability management, software asset management, identity and access management, integration of the Agency-Wide Adaptive Risk Enumeration (AWARE) scoring algorithm, and container hierarchy. Additionally, the ecosystem enables capabilities to support vulnerability remediation and defensive cyber operations.



BENEFITS OF THE ECOSYSTEM

In addition to providing cybersecurity data that leads to improved situational awareness, the CDM Dashboard Ecosystem offers several other benefits, including:

- **Scalability** – Delivery of a data store that has been proven scalable by major commercial users and is capable of effectively handling the large data sets collected across agencies.
- **Performance** – Application of a data store built for speed, allowing rapid query processing and calculation times.
- **Flexibility and Innovation** – Flexibility in the types of products that can be integrated into the solution. This flexibility will open the door to ongoing, innovative, cutting-edge technologies and approaches.

ARCHITECTURE OVERVIEW

CDM Architecture layers A through D represent the flow of data from tools and sensors (Layer A), through a data integration layer (Layer B), to the CDM Agency Dashboard (Layer C), and then summarized and sent the CDM Federal Dashboard (Layer D). The data collected from the tools and sensors of Layer A is integrated and normalized as object-level data in Layer B before it is visualized in the CDM Agency Dashboard. Through cybersecurity posture scoring and prioritization, the Agency users can identify improvements to their cybersecurity posture before they are summarized and reported in the CDM Federal Dashboard at the final layer, Layer D. Through a summarized view of metrics and measurements, the CDM Federal Dashboard users can identify improvements that should be made across the federal civilian government. Data enrichment of vulnerabilities through the integration of threat intelligence feeds and National Cybersecurity Protection Systems (NCPS) provide context for Agency users to make risk-based decisions. The data flow between the CDM Agency and Federal Dashboards is bidirectional, indicating that both dashboards share information with each other. CDM Agency Dashboards send up summary data and AWARE risk scores. The Federal Dashboard sends down Federal Vulnerability Actions (FVA), data about vulnerabilities that is enriched with threat intelligence and NCPS data, and data call/requests for information, etc.).

Notional Vision for CDM Dashboard Architecture