The CDM Playbook: A guide to leveraging CDM for a stronger cyber posture
01 Introduction

Evolving Challenges, Evolving Solutions

Since the Continuous Diagnostics and Mitigation (CDM) program was launched in 2012, the federal IT enterprise has changed dramatically.

We have seen the proliferation of cloud, mobility and related technologies that, practically speaking, have erased the network perimeter and created a much larger threat surface to defend. At the same time, the threat landscape has evolved as well, with the emergence of threats that are more targeted, difficult to detect and capable of doing greater damage.

Fortunately, CDM provides a solid foundation for adapting to this changing environment.

This Playbook
It provides a look at how agencies can leverage CDM to strengthen their overall cyber posture, with a focus on taking advantage of the capabilities that are incorporated in the later parts of the program.

Topics to be addressed include:
- CDM as part of a larger cyber security strategy
- The importance of automation and artificial intelligence
- CDM and the cloud
- The value of CDM dashboards

Each Playbook article offers a summary and key take-aways from a recent blog post.

Additionally, you will find links to a variety of other resources related to the topic.

At Symantec, we understand what it takes to leverage the full capabilities of CDM—not just as a collection of tools but as part of a defense-in-depth strategy that can position agencies to deal with evolving challenges, both now and in the future.
CDM Requires a Holistic Cyber Approach

As the CDM program enters another stage, it requires a new way of thinking, writes Chris Townsend, Vice President of Federal at Symantec. 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 cyber security strategy.

While the first two phases of the program are very much tool-oriented, with a focus on automating the ability to detect the assets and people on a network, the remaining work is designed to deliver more advanced capabilities, including incident response, mobile security, cloud security, network access controls and data protection.

Key take-aways:

• The longer duration of task orders under the final capability areas—as much as six or seven years, versus two or three years in the earlier phases—reflect the greater complexity of the work to be done.
• The new capabilities can only go so far as long as they are deployed as stand-alone functions and not as part of an integrated cyber defense strategy.
• The goal is to identify and mitigate threats to data and applications wherever they reside—whether in the cloud, in on-premise systems or mobile devices.
• In acquiring CDM products and services to address different threat vectors, agencies need to think about how the CDM offerings will work with each other and with other solutions in their enterprise.

Read the full blog post here.

Additional Resources

DHS CDM
DHS provides a concise overview of the CDM program, including a discussion of each of its components.

GAO: Information Security (December 2018)
GAO examines cyber efforts across government, including progress on the CDM program.


Keeping Data in Bound
In this new era of network and data growth, the Department of Defense (DOD) must create a unified DLP policy. Find out why adopting a multi-faceted approach covering several technological domains will be a key component to the DOD’s overall security strategy.
Why Automation Will be Critical to CDM Success

In May 2018, the departments of Commerce and Homeland Security reported that a shortage of federal cyber workers continues to pose a daunting challenge that will only get worse. These findings were not surprising as the government as a whole is struggling with workforce and resource issues. But the challenge is especially pressing when dealing with such a mission-critical issue as cyber security—including the CDM program.

Even if agencies were 100 percent staffed, the tasks laid out in CDM would not be fully achievable. The answer lies in the increased use of automation and artificial intelligence to accelerate CDM processes.

Key take-aways:
The benefits of automation and AI include:

- Faster provisioning of CDM tools.
- Deeper insights through log analytics.
- Better integration with existing security tools and threat intelligence sources.
- Faster response time to security events.
- A simplified investigation process.
- Reduction in time spent reacting to false positives.

Read the full blog post here.

Additional Resources

Press Release: ICD Exchange Simplifies Integration Across Symantec Portfolio and Partner Ecosystem
The initiative covers a wide range of solutions, including SIEM, orchestration, automation and analytics.

Securing Against Malware Using Artificial Intelligence
This blog post looks at how AI can examine the behavior of threats, attackers and system users to predict risk.

Can Cognitive Tools Succeed Where Humans Have Failed?
The security field sees major boon coming thanks to advances in AI, machine learning and advanced behavioral analytics.

The Innovation Imperative: Solutions for the Cyber Lifecycle
This infographic highlights recent advances in cyber security, including the growing importance of AI-based solutions.
How Cloud Computing Has Changed the CDM Strategy

When the CDM program was established in 2012, federal agencies were already in the early phases of adopting the White House’s pivotal “Cloud First” strategy.

While the creators of CDM knew that cloud computing would be a consideration, they could not have envisioned the extent to which the cloud would ultimately alter how government agencies store, deliver and consume information. Under cloud first, security was seen as a unique concern to cloud-related projects, rather than an integral part of an agency’s overall cyber security strategy.

Key take-aways:

• Many applications and platforms that were once siloed are now connected to other systems through the cloud—a fact that must be addressed as part of a CDM strategy.
• Additionally, the combination of cloud and mobility have extended this network outside of the agency to wherever data resides.
• Agencies need to consider end-to-end data loss prevention (DLP) technologies that can protect the data whether it is on-premise, in the cloud, or somewhere in between.
• DLP ensures that data remains secure, while also providing the network visibility required by CDM.

Read the full blog post here.

Additional Resources

Whitepaper: Rethinking Federal Cybersecurity for the Cloud Generation
An integrated, end-to-end cloud security environment can address concerns around data security in increasingly complex environments.

Secure Use of Cloud Apps and Services
This guide discusses the role of CloudSOC CASB Gateway in safeguarding data, protecting against threats and applying controls.

Symantec CloudSOC Data Science for DLP
This brief discusses the role of the ContentIQ data classification engine in identifying and assessing risks to data in the cloud.

Best Cloud Access Security Brokers of 2019 as Reviewed by Customers
Symantec’s CloudSOC was recognized in this year’s Gartner peer insights customers’ choice program.
CDM Dashboards: A Gateway to Better Intelligence

In October 2018, the CDM program reached an important milestone: All 23 major agencies covered under the Chief Financial Officers Act were connected to a cyber security dashboard housed at the National Cyber Security and Communications Integration Center.

The dashboard plays an important role in the CDM process. The data used not only helps federal agencies analyze their own cyber security environment, but it provides the Department of Homeland Security with an extra set of eyes on the federal ecosystem as a whole.

Key take-aways:

- As federal agencies complete each segment of CDM, they gain more and more awareness of the overall state of their network.
- Ultimately, the goal is to turn this data into actionable cyber intelligence that guides fundamental change in network security.
- Data provides valuable information, but intelligence provides the necessary context and technical details surrounding a threat, helping agencies to quickly assess cyber risk and implement proactive controls.
- These dashboards should not stand alone but become part of an agency’s overall security architecture and incorporated into security operations centers.

Read the full blog post here.
06

Why Symantec?

Symantec is the partner of choice for government agencies looking to enhance their cyber posture and make the most out of the CDM program. Our Integrated Cyber Defense (ICD) Platform unifies products, services and partners to drive down the cost and complexity of cyber security, while protecting agencies against sophisticated threats. ICD combines information protection, threat protection, identity management, compliance and other advanced services, powered by shared intelligence and automation across endpoints, networks, applications and clouds, to deliver the most robust capabilities on the market.
For additional information, contact:

federal_government@symantec.com