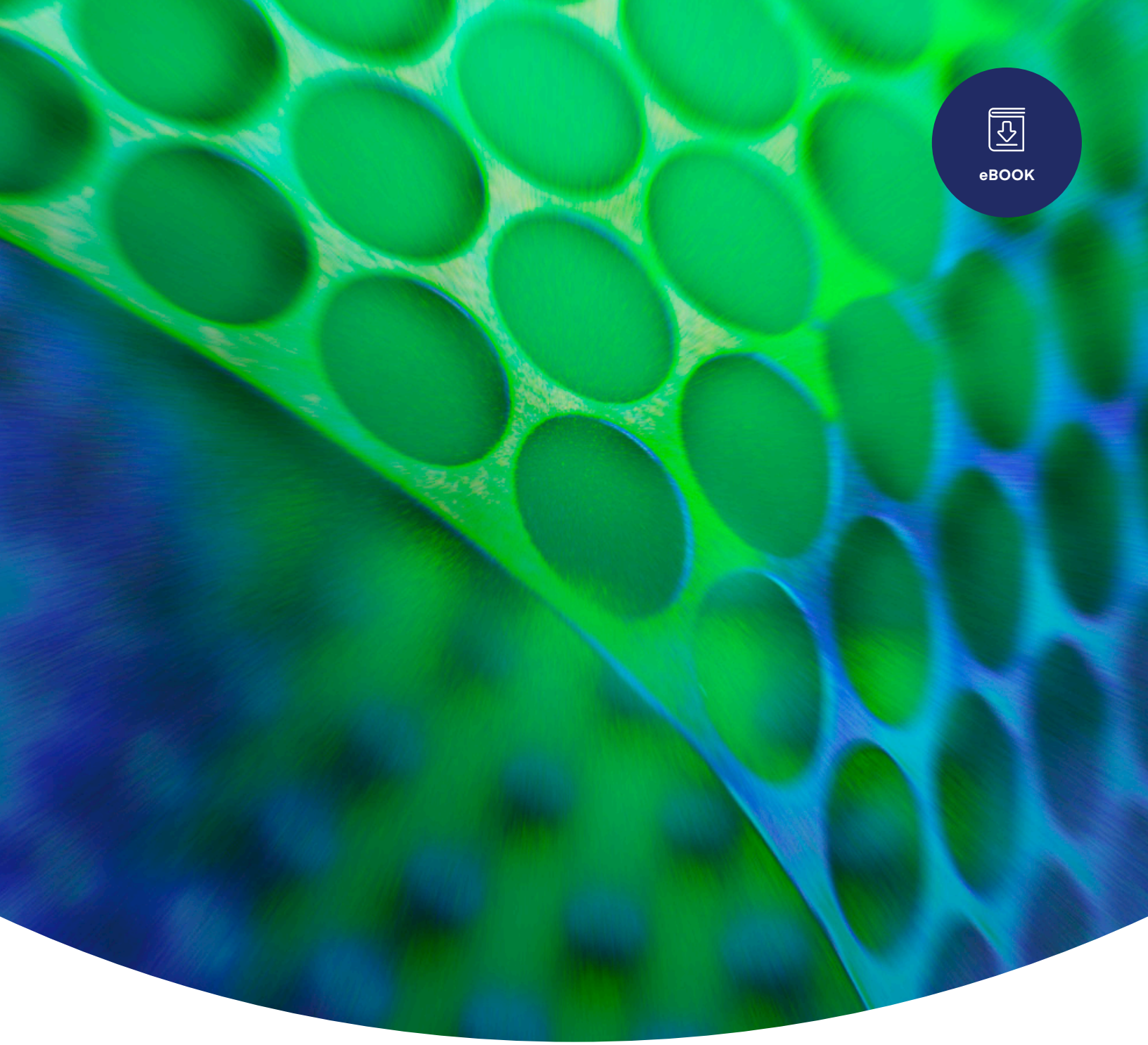


# Closing the Data Breach Gaps with CDM Phase II

SailPoint

As the news of data breaches becomes ever more frequent, federal organizations are arguably under the most scrutiny in relation to their security. And often, the threats have not only come from foreign entities, but also from inside the agency itself – whether the threat is malicious or unintentional. The rampant use of BYOD and cloud computing has made keeping organizations and their data secure only that much more difficult.

While the Federal Information Security Management Act (FISMA) has been one of the main drivers for federal agencies to become more secure, each tackled the directives in their own way, to varying effectiveness. To help combat and prevent the risks associated with cybersecurity, the Department of Homeland Security (DHS) implemented Continuous Diagnostics and Mitigation (CDM).

**Agencies must know, at all times, who has access to their systems.**

CDM is being released in three phases to cover 15 continuous monitoring capabilities that are focused on increasing the security of the systems in federal organizations in a more structured and authoritative manner. While Phase I of the program entailed identifying the current configuration and status of the security systems in place, Phase II is about implementing a governance-based approach to how you control users' access to your systems.

The governance-based approach is one that lets you know at any time "who has access to what," where any aberrant access is not only reported, but also addressed. The organization sees all the relative data to make the right decisions in relation to the access their employees have. Agencies that implement an identity and access management solution can automate a large part of the access certification process and help protect against potential breaches.

At SailPoint, our products specifically address each of the four areas in Phase II of the CDM program, in addition to helping our customers pre-empt potential risks and increase overall security.

**TRUST**
Manage Trust in Those Granted Access

**CRED**
Manage Credentials and Authentication

**BEHAVE**
Manage Security-Related Behavior

**PRIV**
Manage Account Access - Manage Privilege

## TRUST – Access Control Management

In order to keep your data secure, you need to ensure that the right people have the right access at the right time. You must account for joiner and leaver privileges as employees enter and depart the organization, as well as those users who change roles as their time with the organization goes on. It's often found that as employees move in an organization, they accrue access to the different systems necessary to perform each of their different roles. Without a certification process to ascertain who has access to what, this entitlement creep grants the employee access to more systems than they should. In some cases, this excess availability leads to dangerous combinations of access that they might not have otherwise had, increasing the risk for your organization.

**Ensure only properly vetted users have been given credentials, granted access to facilities, systems, information and privileged accounts.**

## BEHAVE – Security-Related Behavior Management

When you employ many disparate systems, seeing the entire security picture is a nearly impossible feat. For continuous monitoring of the controls you have in place for access management to be effective, holistically viewing a users' access is of great importance. For instance, the seemingly innocuous act of a user requesting access to a new system may become more ominous as the approver reviews the other systems to which the user has access. This visibility into critical access-related activities helps prevent behavior that could compromise access into your organizations' systems and prevent data breaches.

**Ensure users meet the security-related requirements for facilities, systems, information and privileged accounts to prevent insider attacks.**

## CRED – Credentials and Authentication Management

When many different systems are employed by an organization, employees' managing of their passwords to those systems can likewise be confusing and complicated. Implementing a single solution that can sync credentials across applications according to your policies not only helps with account lockouts and password resets, but also ensures the systems being used are updated simultaneously without the need for any manual processes. This prevents errant, outdated passwords from being used in between the time the change is requested and then completed in a manual password update task. Provisioning, granting and revoking access to multiple applications and systems within the organization is streamlined as the automation included with an identity management solution can automatically alter employees' privileges as is required throughout their lifecycle.

**Ensure users can be authenticated appropriately and establish if authentication, reissuance and revocation policies are incurring more risk than deemed acceptable.**

## PRIV – Privileges

Granting too much access to users, whether it is at too deep of a level or for too many systems, is an issue that many organizations face. And, entitlement creep creates easy traps into which you can fall. But following and enforcing a least-privilege model, where employees have the minimum amount of access to applications and information necessary to perform their job function, curtails this problem. Defining the desired state access model that employs least-privilege processes through the use of a governance-based approach to identity management reduces the risk of employees' unnecessary access to your organization.

**Ensure that privileges for both physical and logical access are assigned to authorized people or accounts that requrie that access to perform authorized job responsibilities.**

The security of your organization is grounded in managing your risk. An identity management solution, such as one offered by SailPoint, can identify and flag users who are the riskiest, enabling the organization to ensure that those users, in addition to the employees at-large, are granted only the access they need. The holistic view that the right identity management solution can provide makes sure that the breadth of an identity's access is judged throughout the many systems you utilize. Access certifications can be automated to easily manage and monitor employees' identities and access on a continuous basis, allowing for prompt action should any issues arise.

Identity management enforces strong controls across the identity and access management policies and processes that are necessary to meet the CDM program requirements, and more importantly, secure the organization against potential threats.