SailPoint

WHITE PAPER

# Secure Sensitive Government Agency Data with File Access Manager

With the proliferation of filing systems, managing access to data stored in these disparate systems has become a major challenge for government agencies. Over the past few years, the amount of data in file servers, network-attached storage devices, databases, collaboration portals such as SharePoint, and cloud storage systems like Dropbox has increased exponentially — and is projected to grow 800% in the next five years. And it's precisely this data that has become the principal attack vector for cybercriminals.

To address this issue, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which leads efforts to defend the country's critical infrastructure, has put in place a program to strengthen the cybersecurity of civilian government networks and systems, called Continuous Diagnostics and Mitigation (CDM). CDM provides security tools, integration services, and dashboards to participating agencies with the goal of reducing agency threat surfaces, increasing visibility into the federal cybersecurity posture, improving federal cybersecurity response capabilities, and streamlining Federal Information Security Act (FISMA) reporting.

The CDM program delivers capabilities in five key areas: dashboards, asset management, identity and access management, network security management, and data protection management (DPM). DPM focuses on protecting sensitive data – including Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI) – and defines the requirements every agency needs to meet to ensure optimal protection of data and guard against breaches, data loss, and leakage.

## Addressing CDM Requirements

CDM requires the development and maintenance of a Master User Record (MUR) for every person with access to a participating agency network, as well as management of attributes associated with a CDM object. The MUR resides within the associated agency's system and agencies are responsible for protecting the information on them.

In addition, agencies must be able to automatically discover and classify sensitive data assets across multiple applications and environments, as well as label those assets based on the type of data and level of sensitivity so they can be further analyzed, reviewed, and investigated. The classification must be done based on customizable rule-based policies that examine both the content and the metadata to comply with various laws, regulations, and programs. And agencies must be able to secure sensitive data at rest by encrypting, masking, or obfuscating it while also ensuring that proper controls are in place to govern who can access the data.

SailPoint's File Access Manager (FAM) provides a comprehensive approach to help government agencies meet these requirements across all applications and files. FAM delivers enterprise-level identity governance by discovering where sensitive data resides and applying the appropriate access controls. It also provides real-time visibility to improve security, mitigate compliance risks, and support greater efficiency across both on-premises and cloud storage systems.

FAM enables agencies to provide proof of compliance during audits while increasing productivity by reducing time spent on diagnostics, forensics, and data administration tasks. And it simplifies the constant challenge of managing how users are granted access to sensitive files and folders throughout their tenure with an agency.

To prevent the leakage of sensitive data, agencies need to monitor all activities involving that data and be able to respond in real-time to prevent (or abort) unwarranted or suspicious access, as well as isolate and quarantine any compromised information. In the case of an incident, data owners and designated stewards must be alerted and notified, and agencies must secure the uninterrupted flow of communication throughout their security ecosystem to ensure a timely response and minimize the impact and cost of such an event.

SailPoint's solution provides robust capabilities to help agencies maintain complete data-protection CDM compliance at all times:

- **Identify** – Leverage SailPoint's policy-driven Data Classification Engine to automatically detect, catalog, and label sensitive information and metadata, as well as the Entitlement Analytics Engine to get fine-grained access-control views of who has access to that data and how it is being shared internally and externally.
- **Protect** – Enforce continuous governance processes to ensure access controls are implemented, reviewed, and approved in order to reduce the risk of unauthorized access to data. Take advantage of SailPoint's patented Data Owners Election Engine to delegate governance responsibilities and restrict data exposure through role-based access control (RBAC).
- **Detect** – Gain visibility into overexposed sensitive assets, unused resources, access rights, and sensitive data distribution. Identify suspicious and unauthorized activity around sensitive assets and classified data, and aggregate access and usage statistics.
- **Respond** – Automatically perform mitigation and remediation steps to encrypt, archive, tag, or quarantine sensitive data upon detection, and terminate or revoke unauthorized access. Notify admins and owners about data leakage events and report incidents to Security Information & Event Management (SIEM) tools.
- **Recover** – Continuously improve agency data governance and protection compliance posture. Regularly certify access and optimize controls, and report on sensitive data detection, remediation steps, and usage analytics. And investigate incidents and leverage APIs to funnel findings through the entire security ecosystem.

## Responding to Homeland Security Directives

To further manage the risks associated with data protection and governing access to data that resides on governmental networks, the U.S. Department of Homeland Security (DHS), which has oversight of CISA, has defined five functional areas for data protection and governance capabilities: data discovery and classification, data protection, data loss prevention, data leak mitigation controls, and access governance for data.

File Access Manager can help government agencies address these and other critical areas:

### Data Discovery and Classification

Automated discovery and classification is fundamental to implementing controls that restrict and govern access based on sensitivity and risk levels, as well as determining what data should be protected and how it should be protected. FAM's versatile Data Classification Engine delivers an extensive catalog of pre-built policies to address

governmental privacy-related guidelines and applicable regulations (such as HIPAA) while also allowing agencies to create custom policies based on laws, regulations, and program-specific rules (including FERPA).

Agencies can also define multitiered policies and composite rules based on combinations of sensitive data elements to detect, catalog, and label content and metadata — assigning each finding to National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI) categories with an appropriate sensitivity level and exposure risk score. SailPoint's Entitlements Analytics Engine scans through all data assets – both on-premises and in the cloud – and generates a fine-grained view of access controls and shared privileges that reflect how data is accessed and shared, both inside and outside of an agency.

**Data Remediation**

Once sensitive data is detected, automated remediation and mitigation procedures can be triggered to encrypt, quarantine, or archive it. FAM's Data Remediation Engine allows agencies to define rule-based remediation policies based on classification categories, sensitivity level, and risk score, as well as determine desired remediation actions — including file-level encryption, static data masking, quarantining data, blocking access to files, and sending notifications to data owners and security administrators.

**Governance**

Building from a centralized MUR, agencies can extend the capabilities of the SailPoint's IdentityIQ platform and implement a Federal Identity, Credential and Access Management (FICAM) solution that is rooted in governance. FAM extends identity governance to data stored in files across both on-premises and cloud repositories. Furthermore, IdentityIQ and FAM come with a flexible connectivity model and integrated interface that simplifies the management of applications and data in the data center and in the cloud.

File Access Manager optimizes governance processes by automating access certification campaigns and access request flows to ensure proper controls are in place to reduce the risk of unwarranted access to sensitive data. IdentityIQ allows organizations to maintain RBAC to sensitive data, inform governance processes (such as certifications and requests) with sensitivity labels and risk indicators, and ensure access to sensitive data is managed throughout a user's (or an entity's) identity lifecycle.

**Data Ownership**

In many organizations, there is no established framework for the ownership of data stored in files. But this type of framework is essential to the uninterrupted flow of governance, since top-level approaches for data ownership and responsibility can fail or grind processes to a halt. As business users are the ones creating the majority of

this type of information, they often have the most knowledge about the data and who should have access. File Access Manager provides an automated process that uses crowdsourcing to accurately allow those users most active with the data to nominate the true data owner.

**Activity Monitoring**

Securing access to sensitive data is impossible without full visibility and control of that data. To prevent security breaches and theft of sensitive information – or to minimize the potential damage of such activities – agencies need real-time monitoring of identities that access, modify, or transport sensitive files; change file permissions and access controls; as well as the ability to respond to violations.

Information protection labels inform activity monitoring, highlight sensitive content operations, and alert about unauthorized risky access, such as when sensitive data leakage is detected (for example, when sensitive files are shared externally through OneDrive or another cloud solution).

Network telemetry and peripheral data enrich activity information with an extensive auxiliary data and rich identity context. Policies can detect and send alerts about unauthorized access based on user attributes, access attempted from unusual locations (such as at unusual times, from unauthorized IPs or devices, or performing unusual operations that don't conform with the user's identity profile). Advanced activity analytics can detect these patterns and respond to anomalous behavior that could indicate a ransomware attack or other cyberthreat.

**Alerts and Responses**

Response mechanisms allow agencies to take immediate and automated remediation steps to isolate and eliminate threats by terminating operations, revoking access, and quarantining jeopardized data and identities. In addition, built-in integrations can be used to orchestrate protection response, notify admins, and inform any third-party SIEM tools that incorporate FAM into a security ecosystem to increase visibility and ensure communication flow.

**Data Management and Stale Data Detection**

Activity data can also be leveraged for data usage analytics, detecting stale data assets, and revealing unused privileges that can be removed in order to reduce the attack surface and attain a "least privilege" access model. Addressing or archiving unused or stale data can dramatically reduce the risk of forgotten sensitive data being leaked and breached, and can also help agencies reduce costs, expedite data management processes, and prepare for cloud migrations.

**Compliance and Audit Requirements**

Agencies face a variety of compliance hurdles, including the challenge of identifying sensitive information, responding to audits, and maintaining controls around data

access. File Access Manager's forensics and reporting capabilities allow agencies to query and analyze compliance, activity history, alerts, and classification and remediation data to continuously analyze processes, investigate incidents, and improve threat-protection techniques. Built-in integrations and APIs can be leveraged to funnel information through SIEM tools and other monitoring efforts throughout a security ecosystem so insights can be shared to improve the overall cybersecurity posture.

## Achieve CDM Compliance with SailPoint

The Department of Homeland Security has made it an imperative for every government agency to aggregate, correlate, and report the accuracy of its data elements in the MUR. Agencies now have the capability to achieve CDM compliance with SailPoint to increase the efficiency and accuracy of FISMA reporting while dramatically improving their cybersecurity posture. Additional product functionality is available to extend an agency's current FICAM environment and achieve complete governance over privileged and non-privileged users, as well as access to entitlements, applications, and resources.

Part of SailPoint's Identity Security platform, File Access Manager is a powerful tool that can help agencies evolve their overall security posture and achieve CDM goals, including reducing agency threat surfaces, improving agency cybersecurity postures, improving cybersecurity response capabilities, and streamlining FISMA reporting. FAM comes with more than 400 out-of-the-box reports, seamless integrations with SIEM tools such as Splunk and Exabeam, and a wide array of APIs to enable the continuous flow of communication throughout the security ecosystem and aggregate that information into CDM dashboards.

To learn more about how SailPoint Identity Security and File Access Manager can help address CDM requirements visit **www.sailpoint.com/platform/file-access-manager/.**

**ABOUT SAILPOINT**

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting businesses from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their business, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty.



WP1979-2107