



Data Access Governance (DAG)

Datasheet

Benefits:

- Permissions Reporting and Remediation
- Sensitive Data Discovery
- File Activity Monitoring

Introduction

Employees create documents, spreadsheets, presentations, and other files on corporate file shares, Sharepoint sites and in the cloud. Managing and securing this unstructured data poses significant challenges that manual methods and legacy point products fail to address. Modern cyber-security teams seek automated, effective solutions - not standalone technology that must be manually operated. Core Data Access Governance (DAG) provides an automated, scalable, interoperable platform to govern unstructured data. Interoperability with IAM, HR systems, and other applications facilitates automated work flows to secure sensitive data, apply a consistent permissions model and enforce least-privileged access control.



Permissions Reporting and Remediation

Core DAG makes it easy to see who has access to sensitive content or what a particular user has access to across file servers, NAS, SharePoint, Office365, OneDrive, Box, and Dropbox. Risky conditions are flagged in a browser based portal where you can model and simulate permissions before applying to production. The power and flexibility of the platform allows you to set a standard permissions model and apply it uniformly across all access control lists (ACLs).



Sensitive Data Discovery

Core DAG scans the contents of hundreds of document types, even image files using advanced Optical Character Recognition (OCR) technology. Use out-of-the-box rules to meet government and industry compliance standards or add custom criteria specific to your organization's standards. Extend your IAM strategy with an open and flexible architecture. Core DAG seamlessly integrates with your Core Security solutions to extend IAM and entitlement workflows into unstructured data.



File Activity Monitoring



Core DAG maintains a full audit trail of every file touch with all the details. Find out what happened to that missing file or see who's been looking at sensitive content. Activity collection also helps Core DAG identify and revoke stale or excessive permissions without interruption to the business. Core DAG allows organizations to:

- Implement least-privileged access controls
- Track the precise forensic history of file access
- Automate security and compliance policies
- Decrease operations expense and storage costs

Learn More

To learn more about our Data Access Governance solutions, please contact us at info@coresecurity.com or (678)304-4500.

ABOUT CORE SECURITY

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company's threat-aware, identity & access, network security, and vulnerability management solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com