Data Access Governance

Toolkit

Overview

As defined by Gartner, “Data Access Governance (DAG) provides data access assessment, management and real-time monitoring capabilities for unstructured and semi-structured data found in file repositories.” In a world where data breaches are growing both in numbers and sophistication, organizations must do more to protect both their structured (i.e. database-stored application data) and unstructured (file-based data largely stored on the network) data.

Value Proposition

When speaking with customers, use the following statement to succinctly articulate the value that they can expect from the Data Access Governance Solution:

As an emerging part of an Identity & Access Management deployment, Micro Focus addresses the challenges and objectives of the Data Access Governance market through a set of integrated identity-based products that collectively are analyzing, managing, and protecting data for millions of users throughout the world. As a recognized leader in comprehensive data security and management, Micro Focus is uniquely enabled to address the requirements of DAG today and in the future.

Visibility
Gain visibility into data access and permissions

Automation
Quickly provision network access based on identity and role

Protection
Automatically monitor and certify access to high-risk data

Remediation
Meet attestation requirements through data access reviews

DAG Platform Components

Product Name	Technology Overview
File Reporter	File Reporter examines network file systems and delivers the detailed file storage intelligence you need to optimize and secure data for efficiency and compliance. File Reporter provides insight on file and folder metadata, data ownership, permissions, and associated identity information through dashboards, a set of built-in reports, and customized reports. A variety of security reports provides vital insight to who can access what. This data is used for initial correction and policy creation as well as continual assessment. Integrated with both File Dynamics and Identity Governance, File Reporter can produce data be used as the catalyst for remediation and access reviews by business owners respectively.
File Dynamics	Through defined policies, File Dynamics automates an extensive set of network file system management tasks. With File Dynamics you can manage storage provisioning, migration, remediation, and cleanup, along with policy-based protection of high-value file system targets. For DAG, File Dynamics includes a family of security policies that can monitor high-value target data locations and automatically protect against unauthorized security changes and notify data owners of activity.
Identity Manager	Identity Manager powers the entire identity management lifecycle, managing identities and their associated attributes to minimize privileges. This enables organizations to reduce the costs of manual account management and demonstrate compliance while reducing the risk of unauthorized access. Working in concert with File Dynamics, Identity Manager can be the driver for the lifecycle management of unstructured data areas, including access rights to data. See IGA Sales Toolkit here.
Identity Governance	Identity Governance helps organizations run effective access certification campaigns and implement identity governance controls to meet compliance mandates while proactively mitigating risk. The product engages business users in approving, removing, and certifying access to resources. Together with Identity Manager, it is the foundation for a risk-based approach to managing privilege and access. Together with File Reporter, it allows business users to perform access reviews against unstructured Data. See IGA Sales Toolkit here.

Key Messages

Use the following information to begin building your pitch.

#1 –DAG is emerging as a market convergence point for IAM/IGA and Data
We are seeing a convergence in the marketplace with Identity and Data. The governance of access to data is all about Identity and Role appropriately applied to a data security infrastructure. We are involved with Gartner and other analysts to help define and shape this market and have appropriate Gartner reference materials available for support.

Micro Focus is a leader in the IGA market and having a comprehensive DAG offering strengthens that position.

#2 –Sensitive information exists in both structured and unstructured data
Unauthorized access to sensitive information can be devastating. For years, security professionals have advocated the safeguarding of sensitive information such as PII (Personal Identifiable Information) in application databases, but sensitive data also resides in files stored on the network. In fact, with over 80% of an organizations data being classified as unstructured, perhaps this is the most vulnerable.

Organizations likely already have identified or intrinsically know of unstructured data locations that they wish could be more secure such as Finance, Intellectual Property, Legal, or M&A. Micro Focus can help them easily do that.

#3 – Addressing DAG requirements takes a comprehensive strategy, but you can use a phased approach.
Protecting and securing sensitive data requires tools that let you:

- Learn what your users are storing and who has access to it
- Prioritize High-Value (Risk) Target data locations for applying security policy
- Put policies in place that enforce permissions and monitor for unauthorized access
- Conduct periodic access reviews for unstructured data just as we do for application access today

#4 – Getting data owners in the line of business involved is imperative.
No one knows the value and sensitivity of data more than the individuals that work with that data. For legal documents, it's someone in the Legal Department; for financial documents, it's someone in Finance.

IT wants business users to be more involved in the stewardship of their data and the business wants to be more in control of their data.

The Micro Focus Data Access Governance Solution lets you designate data owners from the departments that work with sensitive data to help establish the policies that govern that data. Data owners can help set policies for data access permissions, and be notified when these access permissions have changed or changes have been attempted.

Personas

Having the right conversations with the right people is key in every selling engagement. Use the following information to understand who the File Governance Suite's key buyers and influencers are, their roles, responsibilities, and concerns, as well as suggested conversation topics.

Title	Role	Responsible for	Cares about	What to talk about
CxO (CIO, CISO, CCO)	Buyer Decision Maker Budget Owner	• Protecting business and brand. • Mitigating risk • Compliance	• Identify dark and sensitive data in system repositories to comply with privacy and regulatory mandates. • Improve compliance state and audit reporting across enterprise systems.	• How content can be managed in a secure repository according to policy • Ability to identify sensitive data. • Ability to address identified problems through automated policies. • Ability to secure and protect high-value targets.
Manager	Decision Maker Evaluator	• Applying policy to automate security controls for high-value data locations. • Conducting access reviews for both applications and unstructured data in the network file system.	• Meeting line-of-business concerns around security of data. • Compliance for regulations pertaining to data access. • Using the same tool for access reviews of applications AND unstructured data. • Certification and attestation.	• How File Dynamics family of security policies can be applied to discrete data locations. • How access reviews are conducted using Identity Governance. • How File Reporter integrates with Identity Governance for access reviews to unstructured data.
Data Owner	Influencer	• Identifying who should have access to sensitive data. • Identifying sensitive data.	• Protecting access to sensitive data in his or her department. • Empowered to make decisions when needed.	• Security Notification policies, Lockdown policies, Fencing policies.

Selling Scenarios

When speaking with customers, always tell the whole Data Access Governance story. You should tailor the story to emphasize the benefits to your customers' existing investments.

Technology Deployed	What to Discuss
NetIQ Identity Manager	Identity Manager (IDM) provides the foundation for managing identities and their associated attributes. For IDM customers, you can propose File Dynamics and File Reporter (bundled as the DAG SKU) and Identity Governance. You can also propose a phased approach: • Add File Dynamics for identity-based policies to automatically provision data storage, assign permissions, and control access. • Add File Reporter to gain visibility into who has access to unstructured data. Then review and certify that access through Identity Governance. Review scenarios identified in flyer.
NetIQ Identity Governance	Identity Governance helps organizations gain visibility into who has access to what, driver better access decisions, and demonstrate continuous compliance. Adding DAG means that customers can conduct access reviews on unstructured data stored in the network file system. Most customers who have Identity Governance also have Identity Manager, so it's best to propose both File Reporter and File Dynamics (bundled as the DAG SKU). You can also propose a phased approach, starting with File Reporter. This will enable the customer to scan permissions on unstructured data and import the data into Identity Governance for access reviews.
Micro Focus Storage Manager	Before the introduction of File Dynamics, file management technology for both OES networks and Windows networks was offered in Storage Manager. Many Windows network customers are still running Storage Manager and are unaware that Storage Manager for Active Directory is now File Dynamics. These customers are encouraged to upgrade and to learn how File Dynamics is part of a comprehensive Data Access Governance solution.
Windows Server, Active Directory	File Reporter and File Dynamics (bundled as the DAG SKU) can help you get a foot in the door at prospects who are looking to fill gaps with Windows Server and AD, including: 1) Providing enterprise reporting, rather than single-server reporting offered in the Windows File Server Resource Manager; 2) Reporting on Active Directory, file system metadata, and permissions; 3) Enacting file system actions when Active Directory events take place; 4) Enabling remediating actions though monitoring and the automatic application of policy for things like content control, security, and disposition.

Discovery Questions

The following discovery questions will help you to understand your customers' current situation, identify needs and business issues, uncover competition, and confirm business requirements.

Questions for customers challenged by Data Access Governance

- Are you concerned about risks associated with unstructured data within your organization?
- How do you currently analyze and confirm who has access to high risk data on your network?
- Do you currently monitor and protect the security on high risk data?
- Do you have a need to automate the provisioning and security of sensitive data areas tied to approval processes within Identity Manager?
- Does your company create and maintain high-risk data for customers? How do you provision and secure this data?
- When it comes to security and compliance, what rules or regulations are you required to follow?
- If you needed to identify all of the network folders a particular user has access to, how would you do it?
- How would you determine all of the users who have access to a particular network folder?
- If you were asked in an access review to demonstrate access compliance to unstructured data, how would you go about it?
- For your most sensitive data, how would you be able to learn when access permissions have been changed?

Overcoming Objections

Businesses will inevitably have questions and concerns about any new solution. The following highlights the typical issues that customers could raise and the recommended responses to them.

Category	Customer Objections	Counter Questions	Follow-up Response
Risk	Our access is secured and managed through our identity management system.	Were you aware that with more than 80% of a company's data stored on the network file system, it is perhaps the most vulnerable area for data breaches of sensitive information?	The Data Access Governance Solution can help you identify the sensitive data stored on your network, then automatically secure, move, archive, or delete it. Finally, you can provide attestation through access reviews that only authorized users have access to secure data.
Compliance	We've never had to conduct access reviews to our network data.	Analysts with organizations like Gartner are now recommending that access reviews be conducted on unstructured data repositories.	The Data Access Governance Solution allows you to do so easily using tools you're probably already familiar with.
Complexity	With all of the capabilities that you're talking about, this solution sounds very complex to roll out.	It's common to roll out a solution as advanced as this in a phased approach. Many customers want to first identify their potential access risks through reporting. Does this seem like the right first step for you?	You'll be happy to know that deploying File Reporter is very fast and we can demonstrate potential access risks within a couple of hours.

Competition

The Data Access Governance Solution offers many advantages over the competition. MICRO FOCUS:

- Provides the ability to conduct access reviews for both structured data in application databases, as well as unstructured data residing in the network file system.
- Enables organizations to learn what they're storing and who has access to it, then to establish policies to automatically remediate problems.
- Utilizes Active Directory and, if present, the identity management system to grant and restrict access to network-stored high-value targets based on user identity, role, and group membership.
- Reports on all users who have access permissions to a specific high-value target and how those access permissions are derived.
- Reports on all network folders that a specific user has access to and how those access permissions are derived.

Look for a soon-to-be-published Data Access Governance Solution battle card for more information.

SailPoint

Solution includes: IdentityIQ Provisioning, IdentityIQ Access Certification, and IdentityIQ File Access Manager. The latter was added in order to extend its offerings to Data Access Governance, giving SailPoint a temporary competitive advantage over Micro Focus.

MICRO FOCUS Response

Micro Focus now offers Data Access Governance with the ability to provision, manage and certify data access based on seamless integration with Identity Manager and Identity Governance.

Another important differentiator is that the Micro Focus SRG portfolio provides a comprehensive solution that can meet all the requirements using a single vendor. With SailPoint, the customer will have to rely on other vendors to meet all their security requirements.

VARONIS

Solution includes “DatAdvantage” for “Data Audit and Protection” and “DataPrivilege” for “Access Reviews”. Varonis states that they can synchronize data with any vendor’s IAM solution, allowing them to externally control DataPrivilege entitlement reviews, self-service access workflows, ownership assignment, and more.

MICRO FOCUS Response

The Varonis system is extremely expensive to purchase and deploy. When reviewing the customer's actual reporting requirements, many Micro Focus sales execs have found that Varonis features are nice but not needed.

Unlike the Micro Focus solution, Varonis does not provide an IAM solution and requires complex integration with IAM vendor offerings.

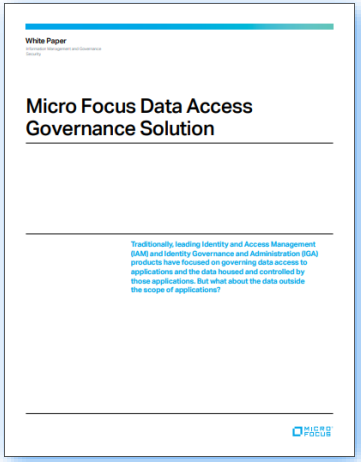
The Micro Focus DAG solution offers a unique ability to provision, manage and certify data access based on seamless integration with Identity Manager and Identity Governance.

Customer Collateral

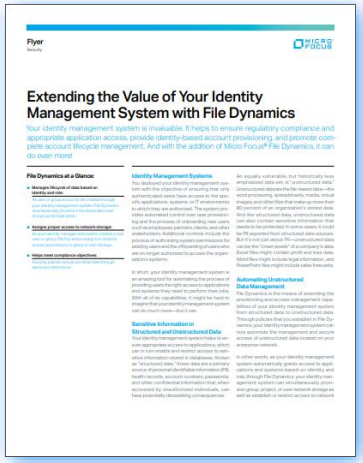
Use the following customer-facing materials when engaging directly with your customers about Data Access Governance. CLICK THE IMAGES TO VIEW.

Flyer: DAG Solution

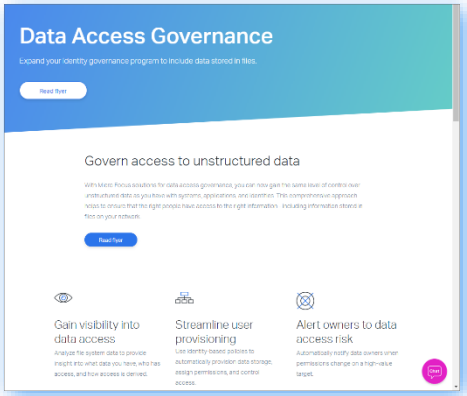
White Paper: DAG Solution



Flyer: Upselling DAG to IDM Customers



Website: DAG Solution



Day 1 Deck: DAG Solution

Resources

Use the following internal materials when engaging directly with your customers about Data Access Governance.

- Sales Enablement Central: NetIQ
- Sales Enablement Central: IMG
- NetIQ Resources Page
- CyberRes Sales Plays
- IGA Sales Toolkit
- Pricing Center of Excellence
- Sales Webinar: Selling File Dynamics to Identity Manager Customers