netgovern™ enforce

AUTOMATED FILE SERVER MANAGEMENT

THE BUSINESS CASE FOR FILE SERVER MANAGEMENT AUTOMATION

Organizations are constantly changing. New hires, staff moving from one department to another, changes to regulations can make it very difficult to see who has access to what file, and to provide appropriate file access. To protect sensitive data, users with varying roles and responsibilities should all have different levels of access rights.

With NetGovern Enforce, organizations can automatically enforce policies and offload the role IT plays in everything from manually managing storage, to information lifecycle management, to protecting and recovering files, or to complying with rules and regulations. By automating file server management with NetGovern Enforce, organizations can ensure tasks will always be performed on time, even if there's a bigger fire burning elsewhere. With NetGovern Enforce, organizations benefit by decreasing the risk of noncompliance and increasing productivity while at the same time reducing data management and storage costs.

FILE MANAGEMENT AUTOMATION AND INFORMATION GOVERNANCE

NetGovern Enforce helps organizations with information governance by reducing manual tasks when it comes to information management. First, records and information management and eDiscovery are improved by the homogeneity and punctuality provided by automation. For example, information lifecycle management tasks regularly performed using the same criteria lower the amount of data stored, facilitates easier search, and reveals better insights as the data is never outdated. The automatic management of sensitive information storage and permission rights also enhances risk management strategies, information security, protection initiatives, and privacy.

TARGET-DRIVEN AND IDENTITY-DRIVEN POLICIES

NetGovern Enforce works with both identity-driven and target-driven policies. Identity-driven policies affect users listed in Active Directory. These policies specify the way user and collaborative storage are managed. They can be enforced on individual users, per work unit, or for an entire organization. Setting the policy once for a work unit in Active Directory automatically applies it to any user residing in the same unit. Target-driven policies affect high-value target data in file servers. Certain actions performed against these targets automatically trigger follow-up actions from NetGovern Enforce. Data Locations, Content Control, and Data Protection are all target-driven policies.

AUTOMATE USER PROVISIONING

NetGovern Enforce connects to both end-user storage and collaborative storage across all file servers. New users added to Active Directory can have their home folders automatically provisioned with the criteria specified in the policies for their organizational unit. They are also automatically provisioned permissions to collaborative storage locations and new storage, profile paths, Remote Desktop Services and their profile paths, and role-specific files.

TAME DATA GROWTH

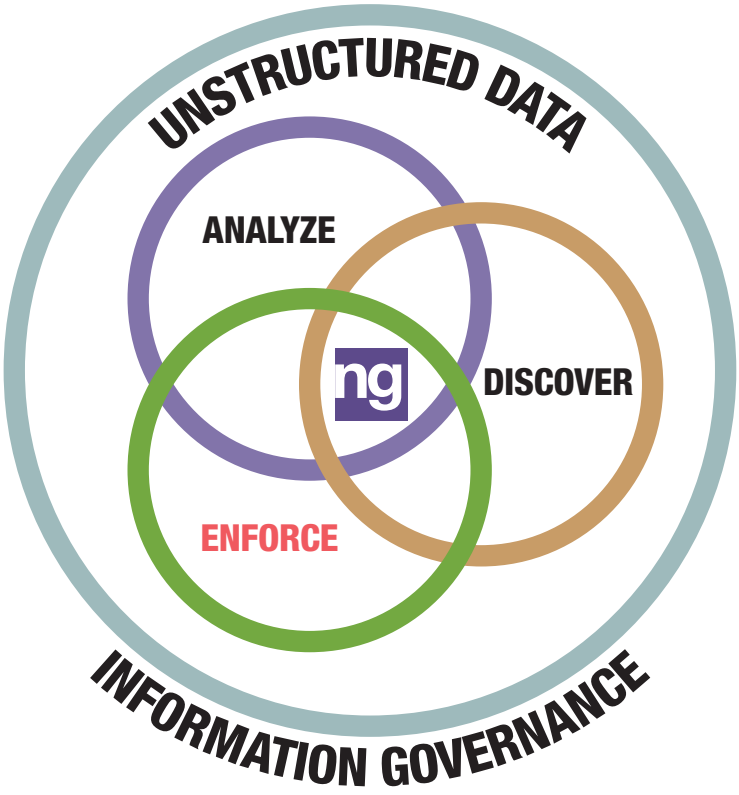
To control data growth, NetGovern Enforce can automatically enforce storage on new users according to their organizational unit. When users are disabled in Active Directory, their home folder can be automatically archived or deleted, and their access rights revoked. NetGovern Enforce also provides tools to remove redundant, outdated, and trivial (ROT) data. Polices can be created to remove files when they meet defined requirements such as folder size, location, permissions, attributes, unallowable file types, redistribution paths, vaulting paths, disposal procedures, and more.

PROTECT HIGH-VALUE TARGETS

NetGovern Enforce automates data protection tasks for business continuity by adding another layer of protection to safeguard data integrity and availability in case of a cyber-attack, file corruption, loss, or deletion. In addition to protecting high-value target files, NetGovern Enforce protects permissions on those files from being lost, destroyed, or altered by mistake. Using a multi-tier approach, both high-target value files and associated permissions are archived as a secondary backup and can be quickly restored to what they previously were at any point in time. This secondary backup is quarantined in a File Store and protected from being accessed or compromised by users.

EASILY MIGRATE USER FILES

File migration can be streamlined with NetGovern Enforce. Moving users in different containers in Active Directory migrates their home folders from the server specified in the source container's policy to the server required by the new container's policy. Distribution settings can automatically migrate user data in other locations while preserving policies to distribute workloads more evenly. Modifying the target path of a policy automatically migrates all of the user's home folders within it.



Visit **netgovern.com** to learn how we help organizations deploy Information Governance software that provides clear answers.

180 Peel Street, Suite 333 Montreal, QC Canada H3C 2G7 • Toll-free: USA & Canada: 1-866-497-0101 • International: +1 514-392-9220 • Email: info@netgovern.com

www.netgovern.com