CONDREY CORPORATION

Bulletin

Securing High-Value Data with Senergy

Target-Driven Security policies in Senergy are engineered to protect your organization's sensitive and high-value data by informing you of changes in access permissions, locking down access to a baseline that is strictly enforced, and providing and denying access based on group memberships.

Data has been called "the new capital." Data drives the decisions of all organizations. It's therefore paramount that organizations protect their data – and especially their sensitive and high-value data – from unauthorized access.

When IT personnel hear the term "data protection" and "unauthorized access," they tend to first think of compliance to regulations mandating that access to records containing Personal Identifiable Information (PII), medical information, etc., be restricted only to authorized users. But an organization's stored sensitive and high-value data is more than PII. It's the financial information located in a spreadsheet, the sales projections to be presented to the board of directors in a presentation file, the details of a merger in a word processing file, and many other files and file types that distinguish the organization or make it competitive.

These file-based examples of sensitive and high-value data are what is known as unstructured data – meaning data that is not structured in a database application. Unstructured data makes up more than 80 percent of all the data that an organization stores. Over time, unstructured data can grow exponentially and without proper vigilance, sensitive or high-value unstructured data files can find their way into storage locations where they can be viewed or shared by unauthorized users.

Fortunately, Senergy from Condrey Corporation has an automated means of protecting your sensitive and high-value data from unauthorized access through Target-Driven security policies.

Senergy and Policy-Based Management

Senergy is a product designed to address the ever-changing definition and requirements of network data management. Senergy does so through policies that take action when an event in Active Directory (AD) takes place, or when you initiate a management action.

Senergy has both Identity-Driven and Target-Driven policies. Identity-Driven policies are assigned to AD containers where users reside in AD and are applied to those users or groups. Target-Driven policies can be assigned to individual storage "targets" such as a Finance folder, or a Marketing share.

Depending on the type of policies that you set up, policies can provision user and group network storage, clean up storage, archive or delete storage, move files, restore files corrupted through ransomware, initiate action from a workload created from another application, protect files from unauthorized access, and much more.

Target-Driven Security Policies

With the objective of providing data access governance to high-value targets located on your enterprise network, Senergy provides a variety of Target-Driven Security policies designed to inform you of changes in access permissions, lock down access to a baseline that is strictly enforced, and provide and deny access based on group memberships.

At the present time, Senergy includes three Target-Driven Security policy types: Security Notification policies, Security Lockdown policies, and Security Fencing policies.

Security Notification Policies

Security Notification policies enable administrators to be notified of any changes in access permissions to network folders. These changes in permissions include a user being given a new or updated permission to a specific folder, or a user has been granted access permissions to a folder by being added to a group.

Notification emails are sent to the specified recipients. Only the recipients that are also Data Owners can log in to the Data Owner Client to view the changes.

Security Lockdown Policies

Security Lockdown policies let you establish the baseline permissions for a high-value target. When unauthorized access permissions are made, the new permissions are removed, and the appropriate permissions are restored.

Updates to security permissions are logged and notifications are sent via email to specified recipients.

Security Fencing Policies

Security Fencing policies set limits on how access permissions may change over time by specifying groups that can be given permissions and others that should never be given access permissions.

Updates to security permissions are logged and notifications are sent via email to specified recipients.

How Target-Driven Security Policies Work

Senergy scans the security of the network file system and records the results to the Microsoft SQL Server database. The first scan is considered the baseline and is the means of comparing changes produced by each scheduled follow-up Security Scan. The Security Scan records the following:

- Discretionary access control list (DACL) of the security descriptor (SD) for the share through which the target path is being accessed
- Owner field of the SD
- Access Allowed & Access Denied (Access Control Entry) ACEs in the DACL

  Inherited ACEs in the DACL are only evaluated on the target path.

  Directly assigned ACEs are evaluated on the target path and all subordinate folders.
- Group memberships in AD for security-enabled Domain Global Groups and Universal Groups
- Local groups on the member server that might have members that reside in an AD domain

How Target-Driven Security Policies Address Changes in Security

Any changes detected result in a security alert to the associated email recipients and notification records written to the database. Each policy type handles these security changes in different ways.

The Notification policy simply records what changed to the database, updates it baseline, and alerts the associated email recipients that there was a change.

The Lockdown policy records what changed along with what action was taken to remediate the changes back to the baseline and then alerts the associated email recipients that changes were made. This baseline scan acts as the baseline, and must be rebuilt when security changes are needed to this associated target path.

The Fencing policy records the security changes identified but applies the rules from the policy to determine if the security changes should be allowed or reverted. If the rules allow for the change, the baseline is update automatically. If the rules do not allow for the change, the change is reverted, and a notification record is created. An alert is sent the associated email recipients that a change occurred.

Learning More

To learn more about Target-Driven Security policies or any of the data management capabilities of the Senergy,

visit condrey.co/senergy

Copyright © 2021 Condrey Corporation. All rights reserved.