SECLORE

Seclore Hot Folder Server

Automatic protection for file servers with best-in-class Data-Centric Security

Key Features

- Protection is pre-defined and automatic
- Security policies are flexible and dynamic
- Data once protected, stays protected
- Seamless access for internal and external users
- Track and revoke access at any time
- Request access from the file owner when a user can't open a file
- Harness the power of the entire Data-Centric Security Platform

File servers are extensively used to store bulk information that is always critical to the organization. These file servers are large repositories of archival data and a mechanism to share data across teams and business functions via shared folders. Shared folders on file servers are commonly used to share files across teams, to share large files that cannot be sent over email, or sometimes just to ensure files get backed up for business continuity and resiliency. Inevitably, these shared folders become a central data repository of business information and grow to become essential for the business to function.

Security and Compliance

While server administrators are pre-occupied with the continuously growing storage needs of these file servers, information security managers face the endless task of auditing, analyzing and monitoring user access permissions. The data is voluminous and includes large amounts of sensitive or regulatory data that could severely hurt business interests if they end up in the hands of an unauthorized user. Ensuring access is limited to the authorized user only, is critical to meet the information security and compliance policies of the organization.

Data Sharing

IT admins can apply a certain level of access control when files reside within shared folders on the file server. However, once an authorized user downloads a file from a shared folder and copies it to the local desktop, there can be no access controls administered on that file from the file server. If the user shares sensitive content with anyone within the organization or even outside, there is no way to trace it, let alone control it. End users often end up violating information security and compliance policies without even realizing it.

Data-Centric Security

Seclore Hot Folder Server allows security policies to be pre-defined for any folder on a file server. Once a security policy is mapped to a folder, the Seclore Hot Folder will ensure that all files saved in that folder will be automatically protected without the user having to do anything.

Granular Usage Controls

Security policies can control:

WHO can access the file?
User or Groups Within or Outside the Organisation

WHAT can they do with it?
View, Edit, Print, Copy Content, Take Screen Grabs, Work Offline

WHEN can they do it?
Automatic File Expiry, Date and Time Ranges, Number of Days from First Access

WHERE can they do it?
Specific Computers or Devices, Specific IP Address

Seamless File Access

Files protected on the file server can be accessed by authorized users via native desktop apps by installing a freely available desktop app for Windows and Mac, as well as mobile apps for iOS and Android devices. Internal users are automatically authenticated via ready to use SSO (Single Sign On) integrations with most of the commonly used Identity Management systems and web-based Identity Federation tools. Users who can't install an agent, can access protected files directly in the browser, including editing and printing, provided they have the permissions.

Persistent Security

Protection controls once applied cannot be removed other than by the original file owner. If any other user tries to copy-paste content from a protected file to another file, or attempts to save a Word file to a PDF or text file, Seclore ensures that the controls persist on the new PDF or text file too. The security of the file stays with the file, wherever it goes and prevents any misuse of the information, either knowingly or accidentally.

File Format Supported

1. Universal Protection controls are enforced on all file formats (excluding executables, scripts etc.)
   - WHO (users, groups)
   - WHEN (date, time expiry)
   - WHERE (locations, devices)

2. Additionally, Advanced Protection controls are enforced on the most commonly used document formats:
   - WHAT (Read, Edit, Print, Full Control)

	**docx, xlsx, pptx, doc, xls, ppt**
	**pdf**
	**odt, ods, odp, odf, odg**
	**txt, rtf, csv**
	**bmp, png, gif, jpg, jpeg, jfif, tiff, tif**

Supported Environments

- Windows Server 2012 or 2016
- Non-windows storage volumes can be mapped on to Windows Servers as NTFS volumes using the iSCSI interface.

Key Features

Protection is pre-defined and automatic

Security policies are pre-defined and mapped to a folder on the file server, to ensure all files saved in that folder are automatically protected. Any pre-existing files also get protected.

Security policies are flexible and dynamic

Folder-level security policies are dynamic and can be changed at any time via a central web-based console.

Data once protected, stays protected

Protection controls are persistent once they are applied to a file and stay attached to the file wherever it goes.

Seamless access for internal and external users

Both internal and external users can access files seamlessly in native apps

Track and revoke access at any time

Trace all activities on sensitive content including who is accessing it, when and from where. At any time, access to the file can be modified, expired or revoked.

Request access from the file owner when a user can't open a file

Built-in workflow to allow a user to request access from the original file owner to handle ad-hoc sharing scenarios.

Harness the power of the entire Data-Centric Security Platform

The Hot Folder Server is a component of the Seclore Data-Centric Security Platform that integrates with a wide array of tools and technologies and ensures enterprise-wide data security and compliance.

Business Benefits

- Bulk data protection is easy and security controls can be easily applied even to large archive data repositories.
- Mitigates the most vulnerable threat vector i.e. the user, by enforcing enterprise security and compliance processes without any dependence on the end user.
- Removes the overhead of extensive end-user training and enablement.
- Security policies are pre-defined at the folder level and get applied even before the data gets shared via the folder.
- Low IT administration overhead of ongoing maintenance and management.
- Low overhead of technology adoption, making it easier to secure large volumes of enterprise information in a relatively short period of time.

USA – West Coast
691 S. Milpitas
Blvd.#217
Milpitas CA 95035
1-844-473-2567

USA – East Coast
420 Lexington Avenue
Suite 300,
Graybar Building
New York City
NY 10170

India
Excom House Second Floor
Plot No. 7 & 8
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072
+91 22 6130 4200
+91 22 6143 4800

Gurugram
+91 124 475 0600

Singapore
Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton
Way
Level 34-01
Singapore – 068811
+65 8292 1930
+65 9180 2700

Europe
Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 7621 5500 350

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

Saudi Arabia
5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

© 2020 Seclore, Inc. All Rights Reserved.

SECLORE