

Seclore FileSecure

Extending Information Security Beyond Your Border



Securing Information Wherever It Goes

**A New Approach to Addressing Your Security,
Privacy and Compliance Requirements**

To effectively function in the business world today, organizations need to share files beyond their perimeter. Currently, the majority of that information is traversing departments and enterprise boundaries without effective controls. Whether it is sharing information with third party partners and outsourcing vendors, utilizing Cloud services such as Dropbox to share files, or downloading files onto laptops and other mobile devices, organizations are losing control over sensitive information. So, how can you encourage external collaboration, safely embrace the use of mobile devices, and leverage cost-saving measures such as the cloud and outsourcing without sacrificing security?

Easily Define, Enforce, and Remotely Control Granular Usage Policies

Seclore FileSecure protects sensitive information regardless of device or location. Whether a file is on a server, in an email, on a mobile device, or copied to a USB Memory Stick unintentionally left behind in an airport, unauthorized users will not be able to access the information. Because usage policies stay with the file, Seclore FileSecure enables organizations to securely adopt mobile devices, Cloud computing and external collaboration.

You can centrally define, attach, enforce, modify, and audit granular file usage permissions including:

Name	Address	Who	What										Delete	
			View	Edit	Print	Copy Data	Screen Capture	Macro	Full Control	Offline	Redistribute			
Head Research FR (Head Research FR@seclogroup.com)			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Head Legal FR (Head Legal FR@seclogroup.com)			<input checked="" type="checkbox"/>											
Head Marketing FR (Head Marketing FR@seclogroup.com)			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Head HR (Head HR@seclogroup.com)			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Head Finance FR (Head Finance FR@seclogroup.com)			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Head Sales FR (Head Sales FR@seclogroup.com)			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Head IT (Head IT@seclogroup.com)			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Head Operations FR (Head Operations FR@seclogroup.com)			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- WHO** they can access it: Users, Teams, Groups
- WHAT** they can do it: Read Only, Edit, Print, Copy, Re-Distribute, Take Screenshots
- WHEN** they can do it: Specific Days, Dates and Times, a Date Range
- WHERE** they can do it: IP Addresses, a Specific Device only, a Specific Computer Only

Granular Control: Easily define and attach granular information-centric usage controls to a folder, file or document.

Secure Information Wherever It Goes

The information usage policies can be easily defined and modified by the document owner or administrator at any time, even after information has been distributed beyond the perimeter. The ability to remotely manage access policies means you can instantly block or modify access to a file as business relationships change or devices are lost. Over 140 different types of files can be "Seclored" including files created by Microsoft Office, Open Office, Adobe, Photos, AutoCAD, and dozens of Text file types.

Here are some of the ways the access and usage policies can be attached to a file:

The screenshot shows an email composition window with a toolbar. A red circle highlights the 'Secure Send' button in the toolbar. The email content includes a logo for 'SECLORE' and contact information for Sapan Sharma, Visual Artist at Seclore Technology.

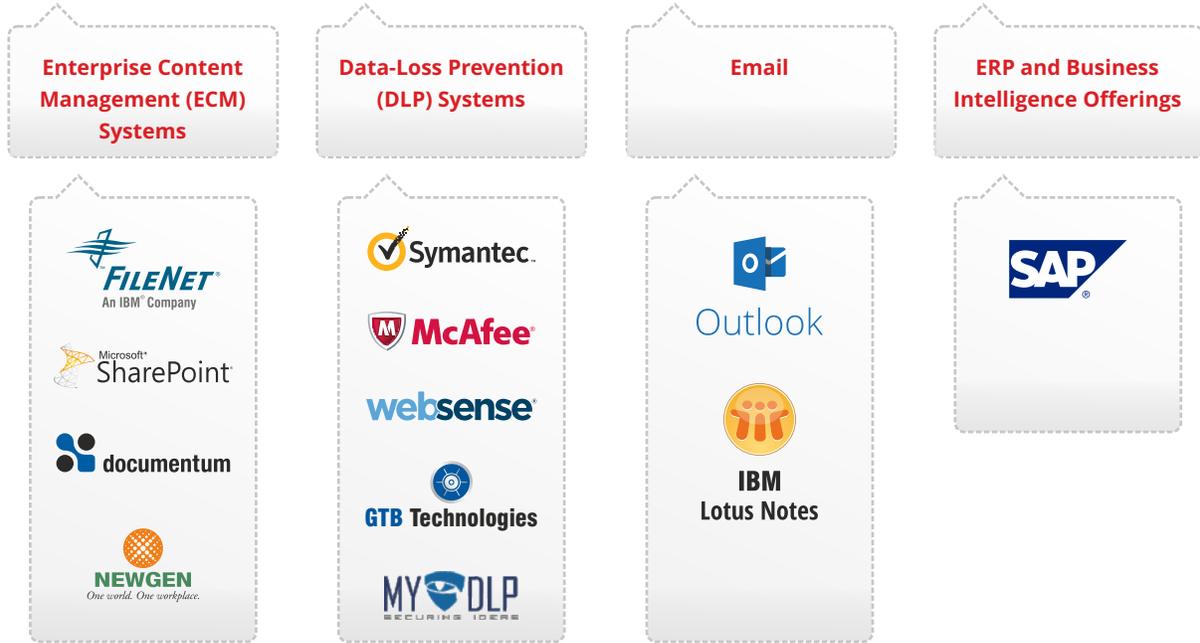
- When a file is closed or saved
- When it leaves the network
- When the file is created based on user-defined prompts
- When the file is attached to an email
- When a file is downloaded from a document management system
- When a file is placed in specially configured "hot folder"
- When discovered by a DLP (Data Loss Prevention) system

Email Protection: A document gets protected along with the email content by using FileSecure's email protection functionality

Extend the Security of ECM, DLP, ERP, CRM, Mail and Messaging Solutions

Seclore FileSecure features a rich suite of pre-built connectors that enable organizations to introduce persistent control over documents as they are downloaded from an ECM system, discovered by a DLP process, or attached to an email.

Pre-built connectors that are available for FileSecure include:



In addition to the pre-built connectors, APIs are also available for easy integration with other core systems including custom and in-house applications.

Simplify Audit and Compliance Reporting

FileSecure features automatic tracking and monitoring of files access and usage wherever they travel or reside. Ready access to consolidated data about who viewed the file, what they did with the file, what device was used to access the file, and when, makes it easy to address regulatory compliance and audit reporting requirements.

List File Activities							
File Activities							
Criteria : 'file id' equals '24'							
<< < 1 [2] 3 > >>							Total : 25
Activity Id.	File Id.	File Name	User	Activity	Date	Authorized?	Mode
131	24	Draft LifeSecure + Plan.doc	Neal-FR	Capture Screen	10 Apr 2010 01:13:48 PM	Y	Online
130	24	Draft LifeSecure + Plan.doc	Neal-FR	Capture Screen	10 Apr 2010 01:13:11 PM	Y	Online
129	24	Draft LifeSecure + Plan.doc	Neal-FR	Capture Screen	10 Apr 2010 01:10:54 PM	Y	Online
128	24	Draft LifeSecure + Plan.doc	Neal-FR	Capture Screen	10 Apr 2010 01:10:02 PM	Y	Online
127	24	Draft LifeSecure + Plan.doc	Neal-FR	Print	10 Apr 2010 01:10:00 PM	N	Online
126	24	Draft LifeSecure + Plan.doc	Neal-FR	Capture Screen	10 Apr 2010 01:09:34 PM	Y	Online
125	24	Draft LifeSecure + Plan.doc	Neal-FR	View	10 Apr 2010 01:09:23 PM	Y	Online
124	24	Draft LifeSecure +	Neal-FR	Edit	10 Apr 2010 01:09:12 PM	Y	Online

Audit Usage of Information:

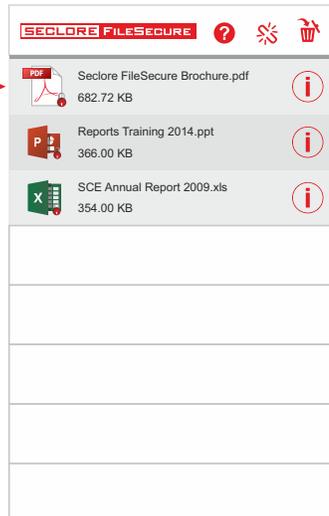
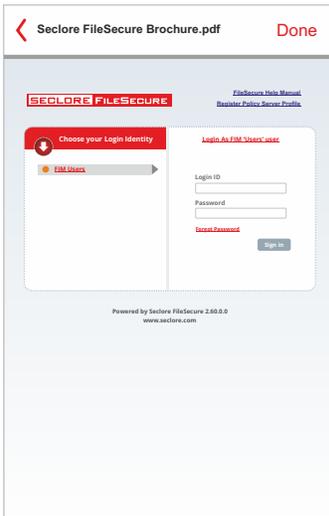
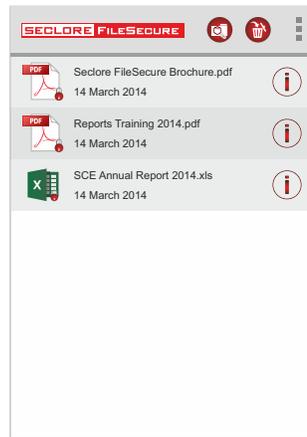
WHO accessed the file, WHAT did the user do, WHEN & WHERE, is all captured from distributed usage environments and reported centrally

Easily Retrieve Protected Documents – On-Demand Viewing

One of the big challenges with information rights management is making it easy for casual recipients to access protected documents. Imagine sharing documents with an investment banker during a merger, or a prospect receiving a proposal; you want to protect the sensitive document without hindering their ability to quickly access and view the protected document.

In addition to the standard client module, which offers full usage capabilities, FileSecure also offers a Lite version for iOS, Android, and Windows devices. The Lite versions enable recipients to access and view protected documents on-demand through a light-weight application.

There is also an agentless, browser-based capability, FileSecure WebConnect, which further ensures your ability to readily share protected documents without impeding collaboration.



Increase Business Agility without Sacrificing Security

The ability to automatically control the usage of sensitive files that move beyond the perimeter of the enterprise will enable organizations to confidently utilize mobile devices, leverage the savings of the Cloud, and embrace external collaboration without sacrificing the security of highly sensitive information.

Customer's Speak

In the world of blurring organizational boundaries and dependence on business providers to process business information, it is imperative for an organisation to ensure that their customer data is safe. Addressing this issue, Seclore FileSecure provided a comprehensive solution to all the information security needs. The software is engineered in a way that it focuses on the 'solution' to deliver business value and not only the "technology".

*CISO,
HDFC Life*

AFCONS Gnosis is like a sanctum within the organisation and whatever gets into the Knowledge Management portal is considered confidential. People have spent years to build this technology footprint and it is somewhat unique to our organisation. To protect this intellectual property, we needed a tool that would facilitate us in giving rights to specific users – something that will allow them to view the documents and not alter, download or kill them. Seclore became useful because once we encrypted the document, it could be decrypted only by an authorised user. And this functionality was extremely useful for us.

*Executive Vice President (Information & Process Management Group)
Afcons*

Among all the evaluated solutions, Seclore FileSecure provided us with maximum flexibility and integration capabilities.

*Senior Manager
Asian Paints*

"We are dependent on different business providers to process our customer information. We still want to control how that information is used and processed by service providers."

*Head of Information Security
HDFC Bank*

The expiry date feature is very exciting, especially when I share documents with outsiders like vendors. The documents automatically lock themselves after a certain date.

*Head of IT
L&T*

About Seclore

Seclore offers an innovative solution, FileSecure, which enables organizations to control access to information wherever it goes, both within and outside of the organization's boundaries. The ability to remotely control who can view, edit, copy, and distribute unstructured information empowers organizations to embrace mobility, Cloud, and external collaboration with confidence. The most integration-friendly solution on the market, Seclore FileSecure extends and enhances the security of information detected and downloaded from DLP, ECM, ERP systems and attached to Mail/Messaging solutions through pre-built connectors. With nearly 4 million users across 420 companies in 22 countries and rapidly growing, Seclore is helping organizations achieve their security, privacy and compliance objectives.

Contact Us

Ready to start securing your information wherever it goes?

Call us at: +1 415 830 6240

Email us at: sales@seclore.com

SECLORE

Securing Information Wherever it Goes

www.seclore.com | info@seclore.com | blog.seclore.com

USA

West Coast

800 West El Camino Real
Suite 180, Mountain View
California 94040
+1 415 830 6240

East Coast

420 Lexington Avenue
Suite 300, Graybar Building
NYC, New York 10170

INDIA

Mumbai

Corporate Office
Excom House Ground Floor, Plot No. 7 & 8
Off. Saki Vihar Road Sakinaka, Mumbai – 400 072
+91 22 6130 4200 | +91 22 6143 4800

Bengaluru

Regional Office
5th Floor, Vakil Square, Bannerghatta Road
Opp. Jayadeva Hospital. Bengaluru – 560 076
+91 97425 11179

Gurgaon

Regional Office
OCUS Technopolis, Golf Course Road
Sector 54, Gurgaon - 122 001
+91 0124 4626 161

