

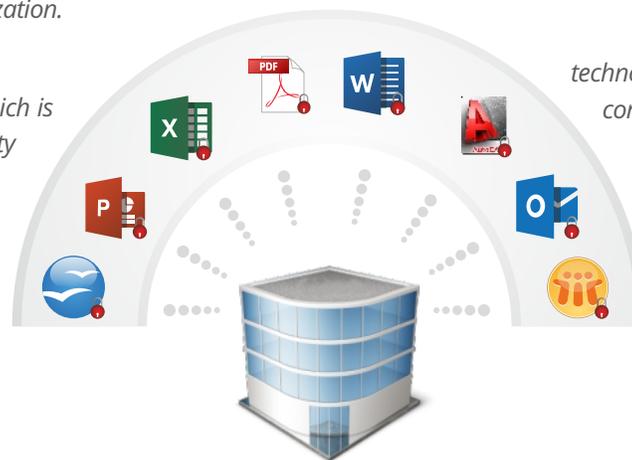
Seclore FileSecure

Information Rights Management

Securing Information Wherever It Goes

Organizations today are increasingly sharing sensitive enterprise data with outside parties such as vendors, partners, contractors, lawyers etc. These entities lie outside your perimeter, outside your control, and outside your security and risk infrastructure. With this increased collaboration however, come increased risks. The shared information – which may include financial data, customer information, technical specifications, engineering designs, etc. - if misused, can have a significant financial, reputational, competitive, and regulatory impact on your organization.

Traditional security solutions focus on securing the enterprise perimeter – which is hardly enough in today's world. Security challenges of perimeter-based security are also deterring smooth adoptions of productivity-enhancing



technologies such as BYOD, Cloud computing, and Mobility. In today's flat, collaborative, and inter-connected world, there is a dire need for security that goes beyond corporate borders.

Security Without Borders: Securing the Message, not the Medium

The most sensitive enterprise information often resides in Word, Excel, PowerPoint, PDF, AutoCAD files or emails – rather than databases or data stores. According to Gartner, around 80% of an organization's information exists in this form - referred to as 'unstructured data'¹. This type of information is extremely difficult to track or control with traditional security tools while it is within the enterprise network, and almost impossible after it goes outside. The external recipients can easily copy, print, edit or forward this confidential data to others; thus posing a grave security risk.

Users – many of whom are not even your own employees but contractors, vendors, partners etc. – are accessing your sensitive information all over the globe in all sorts of ways. What makes it more complicated is the sheer abundance of access modes available to users today: people access your data across different platforms, on different devices, at different locations, in different legal jurisdictions, on different networks, for different purposes – the list is endless. Securing just the perimeter or the device where the data resides is no longer a feasible option. What you

truly need is a solution that secures your information and mitigates your risk regardless of where your sensitive information assets reside – anywhere in the world. After all: how many devices will you control? How many platforms will you secure? How many offshore vendors will you audit?

Seclore FileSecure Information Rights Management

Seclore FileSecure IRM secures information at all times and all locations – regardless of where and how it is stored, transmitted, or accessed. FileSecure protection is completely independent of storage mechanism (File Servers, Endpoints, Cloud, Mobile Devices etc.) and transmission medium (Email, Web, USB Drives, CD/DVD etc.). Thus, your information remains secure at all times and locations – even when it is with a vendor or partner. Your security and risk infrastructure gets extended to wherever your confidential information travels – anywhere in the world.

¹Darin Stewart, Gartner. (2013). Big Content: The Unstructured Side of Big Data. *Gartner's Blogs*. Retrieved from: <http://blogs.gartner.com/darin-stewart/2013/05/01/big-content-the-unstructured-side-of-big-data>

Information owners can determine:

- WHO** can access it: Users, Teams, Groups.
- WHAT** they can do it: Read Only, Edit, Print, Copy, Run Macros, Take Screenshots etc.
- 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.

Important features of FileSecure IRM:

- ✓ **Boundary Independence**
- ✓ **Persistent Protection**
- ✓ **Remote Control Information Access**
- ✓ **End-to-end Monitoring and Auditing**
- ✓ **Agentless Information Access**
- ✓ **Mobile Support**
- ✓ **Remote and Immediate Information Expiry**
- ✓ **Time-based Access Controls**
- ✓ **Location-based Access Controls**

Major Features and Benefits:

Firewalling Information Itself: Complete Independence from Transmission, Storage, and Access Type	FileSecure builds an intelligent security firewall around the file itself that persists with the file regardless of mode of transfer or storage. FileSecure IRM places strict usage controls on information, which virtually eliminates the need for distribution control.
Granular Security	FileSecure IRM allows owners to specify granular usage controls on documents - based on action (viewing, editing, printing, copying, screen captures, macros etc.), time (a number of days or a date range, including instant document expiry), and location (specific devices or computers, IP addresses etc.) for every user or team - and any combination of these.
Remote Control	The file owner can control access to the information even after it has been shared. Access levels for any user can be changed or revoked at any time. The file can also be deactivated – so that it instantly becomes inaccessible to everyone.
Audit Trails	All activities performed on protected files – whether inside or outside the enterprise network - are centrally logged in the system and updated in real time. These logs can be used to create reports to facilitate compliance with regulations and guidelines such as ISO standards, HIPAA, SOX etc.
No Licensing For File Recipients²	You pay only for the users who protect files, not those who receive them.
Agentless Access	Protected information can be accessed in the browser without the need to install any new software.
Mobile Support	Protected content can be accessed on-the-go on iOS and Android devices.

FileSecure Lite for Windows

FileSecure Lite is a light-weight software that can be used to view and print protected files on-the-fly. It does not require any administrative privileges to install. Installation and rollouts are quick and easy. It also enables you to view protected files without any native application installed.

File Format And Application Support

Support for over 140 file formats and a wide range of applications, ranging from Open Office to AutoCAD. MS Word, Excel and PowerPoint formats, PDF documents, CSV files, Image files are supported. FileSecure also supports all common applications for opening protected files such as Microsoft Office, OpenOffice, Adobe Reader etc.

²Not applicable for selected cloud-based deployments.

Seclore FileSecure possess numerous features that facilitate safe and convenient external collaboration:

- No Licensing For File Recipients
- Mobile Support For iOS And Android Devices
- No Local Software Installation Required For Information Access
- Light-Weight Local Agent Available That Installs Without Administrative Privileges
- Offline Authentication And Authorization
- Support For Federated Identity Management Systems And Multi-Factor Authentication
- Keys And Content Always Kept Separate
- Centralized Policy Administration

Offline Information Access	Protected content can be viewed in offline mode the same way it is viewed while online – with the same access restrictions in effect. There is no difference in user experience in the two modes.
Email Protection	Protected emails can be sent directly from within the email client. Emails and attachments are protected on the fly just before sending the email. Such emails cannot be read by unauthorized recipients if they are sent or forwarded to them – accidentally or maliciously.
Separation Of Keys And Content	The decryption keys for protected files do not travel with the file itself but are stored in a centralized database. Content is encrypted in its original location. No content – encrypted or unencrypted - travels to the FileSecure servers. All keys are secured throughout the lifecycle - on end user devices, the network, and the server infrastructure.
Support For Multi-Factor Authentication	FileSecure supports multiple authentication factors for both internal and external users. These can be software-based factors (eg. A one-time password (OTP)) or a hardware-based authentication mechanism, such as a USB dongle or a fingerprint scanner.
No Change In Default Application	Protected files open in the native application. For example, a protected doc file will open in the default application set by the user – whether MS Word or OpenOffice.
Retention Of File Format, Name And Extension	There is no change in the file format, name, or extension of a file after protection.
Centralized Policy Administration	Administrators and business heads can create predefined FileSecure policies for protectors to use while protecting documents. Protectors can be restricted from creating their own policies.
Pluggable Encryption	Seclore FileSecure is shipped with high-performance AES 128 and RSA 2048 encryption technologies. However, FileSecure can also use custom encryption algorithms to encrypt protected files. Organizations can define what level of encryption they need for their information.

Seamless Integration with Enterprise Systems

FileSecure IRM is capable of existing as an infrastructural element - a full-fledged layer in an organization's IT infrastructure. FileSecure IRM is pluggable into any enterprise software such as Identity and Access Management (IAM) systems, Single-Sign On (SSO) systems, Enterprise Resource Planning (ERP) systems, Enterprise Content Management (ECM) systems and Document Management systems (DMS), Data Loss Prevention (DLP) systems, Security Information and Event Management (SIEM) solutions, other Transactional systems, Email and Messaging systems etc.

FileSecure IRM policies can be attached to a file:

- Based on user-defined prompts and actions
- When it is created or saved
- When it is dropped in a particular folder
- When it leaves the enterprise network
- When it is attached to an email
- When it is downloaded from an ERP, DMS, or ECM system
- When it is discovered by a DLP system