



SECLORE

Borderless Security

SECURE OUTSOURCING

EMAIL SECURITY

INFORMATION RIGHTS MANAGEMENT

DOCUMENT PROTECTION

REGULATORY COMPLIANCE



Do you receive confidential information (and the associated liability) from customers?

Confidential, personally identifiable information received from customers comes with the liability of revenue and reputation loss in case it gets leaked from within your enterprise.



Seclore FileSecure enables you to control information received from customers to specific people and specific usage, thus increasing accountability of information usage and providing comfort to your customers.



Do you send confidential information to vendors?

Typically confidential information sent to vendors is governed by non disclosure agreements without a mechanism to enforce or track the agreement. Therefore you are dependent on the vendors' systems and processes for the confidentiality of your critical information. Loss of information from the vendor could lead to reputation and legal risks for your enterprise.



Seclore FileSecure enables you to control the usage of information sent to vendors and prevent unauthorized viewing, printing, editing and distributing of the information. Information can also be remotely made unusable in case the relationship ends.

Do you generate revenue by providing reports & other information?

Information and reports sent to one “paid” customer typically lands up with multiple people and enterprises leading to many “unpaid” customers. Revenue leaks thus caused directly affect the bottomline of the company.



Seclore FileSecure prevents revenue leakage of documents and reports by restricting unauthorized viewing, copying and distribution, thus driving revenues and preventing piracy.



Do you frequently establish temporary/project-based relationships with partners and contractors?

Temporary relationships with partners and vendors for a specific project typically leads to extensive information sharing during the execution. After the project ends, the information and intellectual property shared continues to be retained and used by the partner, sometimes against the enterprise, leading to financial losses.



Seclore FileSecure enables you to “retract” information shared with business partners after a specified period thus protecting intellectual property and driving revenues.

Do you have confidential information which only a specific group while in employment, should use?

Research data, business plans, forward-looking financial statements and MIS reports are just some examples of information which are best used only within the walls of the enterprise. Malicious intent, errors and omissions and lack of awareness could make this information publicly available leading to potential losses.



Seclore FileSecure protects information from leakage due to malicious intent, errors and omissions, as well as lack of awareness, by providing a persistent, information-locked method of protection. This means that confidential information remains confidential post distribution.



Do you need to monitor the flow and usage of confidential information for compliance to SOX, ISO, PCI, etc.?

While GRC technologies and processes effectively monitor and control access rights within applications and folders, they do not effectively track the flow and usage of unstructured information in the form of documents and emails. Confidential information traverses department and organization boundaries in unstructured forms without effective controls or monitoring of its use.



Seclore FileSecure provides comprehensive and detailed audit trails for information usage including the WHO, WHAT, WHEN and WHERE of the usage. This includes authorized activities and unauthorized attempts. Compliance costs can significantly be reduced by using these out-of-the-box reports.

What is Seclore FileSecure

Information and its control typically flow together. The only way of restricting control of information and its use, is to control its flow. Enterprises are faced with the tough challenge of sharing information and inviting the risks of information breaches or not sharing information. This open information sharing often leads to information breaches. Seclore's technology allows digital information and its control to be unique and separate. Information that is sent out can be remote controlled. It can be made to become un-printable, un-editable or self destruct. Remotely.

Seclore FileSecure enables enterprises to mitigate the risks of information breaches by allowing people and enterprises to distribute information freely but retain control of the information irrespective of its location or method of transmission.

Files shared can be controlled for access to the documents in various forms.

Control Who Information owners can control who can use the information i.e. people, groups...

Control What Individual actions like read, edit, print, distribute, can be controlled

Control When Information usage can start and stop based on time i.e. dates, timespans...

Control Where Information can be locked to networks and locations i.e. office, branches, specific customer locations.

Seclore FileSecure uses military grade encryption technology to encrypt information and applies information-owner-controlled "usage rights" on the information before and after distribution. Since the rights travel with the information itself there are no risks of information leakage by transmission and copying of the information.

“ *The traditional approach of information security has taken a very wide focus at protecting enterprise systems, often at the expense of the data and information contained within.*

– Gartner, 2009

”

“ *40% of an average enterprise's sensitive data is estimated to be in unstructured formats, (PDFs, MS Office formats, email, webpages). The biggest challenge with protecting and managing unstructured data is that it has become so important, and so easy to share.*

– Aberdeen Group, 2009

”

“ *Confidential data held by businesses and other organizations has never been more critical or less secure, especially in light of the trend to outsourcing and offshoring. The consequences of data loss — compromised commercial strategies, financial liability, tarnished brand image, violation of government regulations and more — are better understood.*

– ABI Research, 2009

”



SECLORE

Seclore Technology (incubated and promoted by IIT, Bombay) is a leading provider of information security solutions in the areas of information usage control, information rights management (IRM) and secure outsourcing. Its expertise lies in protection of data post distribution irrespective of its location or mode of transfer.

info@seclore.com

Blog: blog.seclore.com

Join the Seclore group on LinkedIn <http://www.linkedin.com/e/gis/1136837>

www.seclore.com



SECLORE