

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





What happens to your “paid” research reports and data after you have sent it to customers? 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 bottom line of the company.

SECLORE FILESECURE

Share with Confidence !

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

Seclore FileSecure allows enterprises to define and implement information usage policies. A policy is an "answer" to four Questions i.e.

🔒 **WHO** can use the information

People & groups within and outside of the organization can be defined as rightful users of the information



🔒 **WHAT** can each person do

Individual actions like reading, editing, printing, distributing, copy-pasting, screen grabbing etc. can be controlled



🔒 **WHEN** can he use it

Information usage can be time based e.g. can only be used by Mr. A till 25th Sept or only for the 2 days



🔒 **WHERE** can he use it from

Information can be linked to locations e.g. only 3rd floor office by private/public IP addresses



Besides controlling information usage Seclore FileSecure also provides detailed audit trails of information usage as it travels outside of the organization and can help getting insights into information usage patterns.

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.



SECLORE