SECLORE™

Data-Centric Security for Financial Services

Know, protect, and control your most sensitive digital assets wherever they go.
Close your data security gap and prevent data theft and achieve compliance with Seclore.

$885M

Total (USD) of the top three fines across capital markets firms in 2022

CSO Online

The Challenge

Sensitive digital assets are shared with limited visibility, security, and control, exposing financial services firms to the risks of regulatory fines, reputational damage, lawsuits, market reaction, and high incident cost.

What Do Leaders Need to Do to Protect Their Organizations?

Illustrative Risk	Prevention
Client confidentiality breaches	Know and track whom within the bank and third parties have access to client PII data, as well as the ability to recall or revoke access on demand.
Financial exposure and reputational damage	Gain insights into and protect the integrity of the trade and counterparties associated with bilaterally uncleared OTC derivatives to prevent financial exposure and reputational damage.
Insider trading	Set controls and make material non-public information (MNPI) available and accessible to only authorized users on the buy & sell sides to prevent inadvertent wall-crossings.
Leakage or theft of sensitive data by third-party vendors	Validate third-party vendor access and entitlement levels and mitigate unauthorized and unwanted access attempts.

What Are Leaders Experiencing?

87%

Say that sensitive information sharing happens ad-hoc, outside applications & systems

92%

Say there is no mechanism to know access and entitlements to the sensitive information within and outside of the firm

94%

Say there is no way to take action by electronically recalling or revoking access to the sensitive information, once shared

84%

Say it is hard to prove compliance to policies, standards, and procedures

96%

Say incident response costs are high and cause disruption

Know, Protect, and Control Your Organization With Data-Centric Security from Seclore

Know

Exactly what's shared and where your data is

- Risk insights & trends
- Access patterns & usage analytics
- Location awareness

Protect

Every single asset wherever it goes

- Policy management
- Dynamic watermarking
- Classification labeling
- AES256 bit encryption

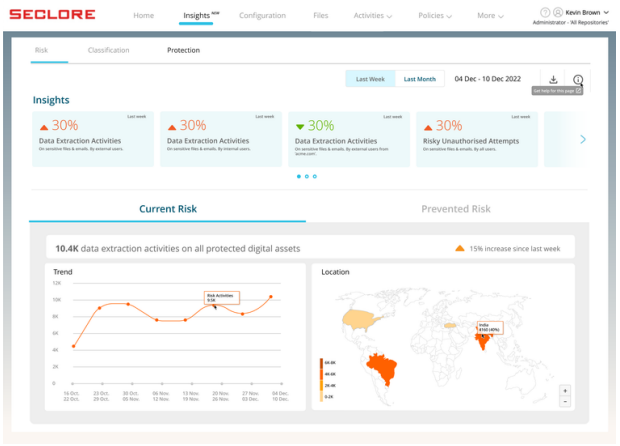
Control

Who has access and revoke it at any time

- Granular access control
- Real-time access revocation
- Dynamic policy federation

Prevent Data Theft & Achieve Compliance

Seclore embeds security controls into the data itself so that it is protected, revokable, and auditable regardless of the device, network, or application – for every digital asset, wherever it goes.



With Seclore, Financial Services Firms Can:

Securely collaborate – Internally and externally on a need-to-know basis

Gain visibility – Where and how your sensitive data is used

Reduce incident costs – Driving down the impact and containment

Mitigate risks – Human error, control gaps, or malicious intent

Achieve compliance – Internal and regulatory policies, standards, or requirements

Make data security independent – Separate from infrastructure security

Securing Digital Assets Across

Any User | Any Device | Any App | Any Cloud

Third-Party Risk • Insider Threat • IP Protection • App/Cloud Data Security • Data Privacy

About Seclore

Protecting the world's sensitive data wherever it goes. Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance. Our data-centric approach to security ensures that only authorized individuals have access to sensitive digital assets, inside and outside of their organization. Enterprises can set automated policies and enable users to control and revoke who has access, what access they have, and for how long. Learn why leading enterprises like American Express and Applied Materials choose Seclore to protect and control their digital assets without sacrificing seamless collaboration and data sharing.