Seclore Data-Centric Security Platform

Close Your Security Gaps with Data-Centric Security

Introduction

Your data is in constant motion. Once it leaves your enterprise–whether shared with a trusted third party or leaked–it's out of your control. Traditionally, we've taken a perimeter-based approach to security, thinking that if you can control the furthest-reaching parts of the enterprise–the "perimeter"– everything inside will be safe. But business has modernized. With forces like remote work, cloud adoption, and the reliance on third-party partners, it is no longer possible to contain data within our four walls. Your business relies on the ownership, storage, and transfer of digital assets to exist and grow. You don't want them to fall into the wrong hands.

Data encryption has long been a proven means for protecting vital data, but it has limitations. Encryption is a blunt instrument that often adds unnecessary hurdles to the data flow. Once decrypted, data can be easily leaked.

Reactive controls, such as data loss prevention (DLP) and cloud access security brokers (CASB), can also help protect data. However, these tools are often cumbersome to deploy and must be faster to be effective. They can only do a little to protect shared data outside of an organization's immediate control.

Many organizations are looking at how to build a Data-Centric Security infrastructure to efficiently eliminate security gaps, especially in light of privacy regulations. Regulations such as GDPR, NIST, CCPA, etc., require sensitive data to remain protected, whether the data is in your custody or the custody of an authorized third party.

Achieve Data-Centric Security

Data will continue to be the increasingly valuable lifeblood of any organization. To protect this valuable asset, organizations must think differently about data protection. Rather than relying on the traditional boundaries of networks and devices, organizations must move the security and control to the data itself. By embracing data as the new edge, organizations can create a boundary around their data that carries and maintains usage policies and security controls. The Seclore Platform provides a data-centric approach to security, enabling you to achieve your key business objectives.

Enterprises can accurately classify, protect, track, and control every digital asset–secured using the Seclore data-centric security platform. The capabilities enable enterprises to know, control, and protect their data wherever it goes to prevent data theft and achieve compliance.

The Seclore data-centric security platform enables you with:

- Risk Insights: Gain visibility across all your digital assets for insight into risk and threats of non-compliance.
- Digital Asset Classification: Determine what data you own and classify how confidential it is.
- Digital Rights Management: Set dynamic enterprise-level policies and granular user-level permissions to control who has what access to which digital assets.
- Tracking & Reporting: Track and report how sensitive data is being used, whether it resides in your vendor or partner networks, public networks, the cloud or on mobile devices.
- Automation Connectors: Leverage existing enterprise systems to automate protection and tracking
- Security Orchestration: Embed security in the business workflows and automatically collaborate securely through Seclore's integration of email, file servers, Microsoft 365 etc.

* Integration with ID, Discovery, Classification, SIEM

** Email, cloud and on-premise repositories/ collaboration

Risk Insights: Expand the Visibility of Sensitive Assets and Provide Insights

Visibility of Risk & Data

Seclore Risk Insights provides enterprise-level visibility and insights for their most sensitive digital assets, such as intellectual property, sales data, and personally identifiable customer information.

Security and Risk Management (SRM) leaders are more aware of the risk exposure and the quantum of risk averted with Seclore.

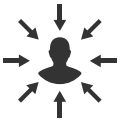
Insights That Drive Action

The Risk dashboard automatically tracks and monitors files' access and usage wherever they travel or reside. It also provides access to consolidated data about who viewed the file, what they did with it, the device used to access it, and when makes identifying opportunities to mitigate risk quickly.

SRM leaders will be able to know where the issue lies and take action either through Seclore or other ways.

Digital Asset Classification

Multiple products work in silos where you must define classification policies or rules separately and the protection rules separately. Seclore is a single product providing all the capabilities with a single console. Seclore Digital Asset Classification allows you to classify documents and emails within the application or on the desktop. Based on the classification label applied, automatic rights management protection controls will be applied to those documents and emails.



User-Driven Classification

User-Driven Data Classification allows users to apply a sensitivity label on the document or email based on security requirements. Visual markings in the header and footer are applied to the email or document.

Classification-Driven Automatic Protection

Seclore Digital Asset Classification allows you to apply a sensitivity label to documents, which can be either user-driven or based on the discovery in use. So whenever you access documents or emails, it can automatically look for sensitive information and apply the right labels. So based on the classification, not only the labels or visual markings applied, but automatic protection comes into the picture with a single rule engine.

Reporting Classification Activities

A reporting console with a complete view of the classification activities and the right set of protection controls applied for this classified information.

Enterprise Digital Rights Management

Seclore's Enterprise Digital Rights Management, in combination with Digital Asset Classification and Risk Insights, enables organizations to automate the end-to-end data-centric security process, from classification to protection and usage tracking.

Organizations can verify who can access their data and apply fine-grain and dynamic policies to ensure only authorized users can access it. Furthermore, organizations can confidently revoke access rights when no longer needed or if circumstances change—regardless of where the data is located—eliminating the common challenges of "all or nothing" access.

Tracking and Reporting

Seclore tracks and delivers intelligent insights into the usage of sensitive data, whether with your vendor or partner networks, public networks, the cloud, or on mobile devices. Authorized actions and unauthorized attempts are automatically tracked and collected. The owner can receive document usage alerts and view and analyze insights on the Seclore Dashboard for easy viewing and analysis. In addition, the solution can export document usage activity logs to a SIEM system. The aggregate of the information provides significant forensic and usage trends, as well as streamlined audit and compliance reporting.

Seamless Integration of Best-of-Breed Technologies

Seclore's data-centric security platform seamlessly integrates DLP, Data Classification, Rights Management, and SIEM systems to build an ironclad data-centric security framework that leverages metadata to automate processes between the systems. This tight integration provides the flexibility to leverage existing best-of-breed solutions while allowing you to future-proof your infrastructure for new, innovative data-centric security technologies.

Automation Connectors: Leverage Existing Enterprise Systems to Automate Protection and Tracking

The Seclore Data-Centric Security Platform also makes adding data-centric security to existing content management, email, and file-sharing systems accessible through a library of connectors and integrations. These integrations automatically apply granular usage controls to documents as downloaded and shared, ensuring sensitive information is consistently protected and tracked.

Security Orchestration: Map Policies and Identities from Third-Party Systems for Easy Implementation

Two powerful capabilities, Identity and Policy Federation, are also part of the Seclore Platform. Identity Federation makes it easy for internal and external users to authenticate to ensure adoption and use. Policy Federation reduces administration costs and sets the stage for automation by mapping policies from other systems (e.g., ECM, ERP, Data Classification, DLP, EFSS) to the granular usage controls in the Seclore Data-Centric Security Platform.

Conclusion

The Seclore data-centric security platform provides end-to-end and holistic security to data, right from rights management to integration with collaboration applications. The recent enhancements in Digital Asset Classification (DAC) and Risk Insight Dashboard raise data security by several notches. As a result, enterprises now have more control and visibility over their data.

Contact our team for more information about Data-Centric Security.

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. Visit www.seclore.com for more information.

SECLORE™

www.seclore.com
info@seclore.com