SECLORE

Seclore SDKs

Extend the Power and Value of your Security Software Offerings and Enterprise Applications with Data-Centric Security

Overview

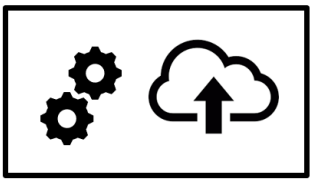
To support security software solution providers and organizations who want to add data-centric security to their business and transactional applications, Seclore has created comprehensive Software Development Kits (SDK). The Seclore SDKs features a robust collection of APIs and rapid configuration capabilities that reduce the effort required to add persistent, granular usage controls and tracking to information as it is discovered, downloaded, classified and shared. By adding data-centric security to an application, information remains under the organization's control – even when it leaves the application and moves beyond organizations' boundaries.

There are two primary SDKs available from Seclore: The Seclore Server SDK and the Seclore Endpoint Auto-Protector SDK. The Seclore Server SDK is designed to support the integration of Seclore with enterprise applications that run in the background The Seclore End-Point Auto-Protector SDK, a configurable cross-platform tool, makes it easy to add data-centric security to solutions that run on end-uses devices.

Types of Applications Supported by the Seclore SDKs

Seclore Endpoint Auto-Protector SDK

- Supports Applications that run on End-Users' Machines (e.g. Endpoint DLP, Data Classification, Data Governance)
- Runs in User Context
- Cross-Platform Endpoint Auto-Protection (Supported on Windows and Mac)
- Configurable for Rapid Integration



Seclore Server SDK

- Supports Applications that run in the Background (e.g. Business & Transactional Apps, Network DLP, Email DLP, CASB, Content Collaboration Platform (CCP), SIEM Tools, e-Discovery)
- Support for Multi-Tenant Applications
- Available in Java and .Net

Key Capabilities

Extending Data Protection Beyond Security Software Solutions and Business Applications

Integrating the Seclore Server SDK with an enterprise application will keep data under the organization's control – even when it is shared externally. Seclore can seamlessly take over where the enterprise application's protection ends – adding persistent granular usage controls and tracking that stay with the file wherever and however it travels. The Seclore Endpoint Auto-Protector SDK enables vendors providing DLP, CASB, eDiscovery, and other endpoint-based security solutions to add rapidly add the capability to automatically protect information as it is detected.

Robust APIs

The Seclore SDKs offer a complete set of RESTful APIs as web services with supporting documentation and sample code to make service calls from any platform or device. All calls are secured via built-in authentication controls and all communication happens using secure protocols.

Configurable Endpoint Auto-Protector

Leveraging the configurable Seclore Endpoint Auto-Protector SDK, documents can be automatically protected as they are discovered and classified. With the combination of technologies, organizations will be able to protect and track information wherever and however it travels. To streamline deployment, the Seclore Endpoint Auto-Protector SDK comes built-in with the Seclore Agent, removing the need to ship the SDK separately on the endpoints.

Automated Protection for Service Applications

Through the integration with the Seclore Server SDK, documents can be automatically protected as they are downloaded from or uploaded through any server application – without any end user intervention. The addition of persistent, granular usage controls gives organizations the ability to control and track the use of information wherever it travels as well as streamlined compliance reporting.

Identity Federation

To ensure a seamless experience for the end-user, Seclore provides a robust Identity Federation capability. The result is that end users can authenticate using the organization's existing Identity and SSO solutions. Identity Federation is achieved by integrating with Identity and Access Management (IAM) and SSO systems to provide the same experience for user authentication. Seclore has readily available connectors for most Identity and SSO solution providers including Microsoft Active Directory, IBM Tivoli Directory, Domino LDAP, Sun ONE LDAP, Google Authentication, and more.

Content Inspection of Protected Files

Using the Seclore SDKs, business applications, DLP, CASB, Data Classification, CCP and more, can be readily integrated with Seclore Data-Centric Security to automatically inspect content or leverage the application rules for automated protection.

Policy Federation

Seclore Policy Federation makes it easy to map an application's access policies to Seclore's granular usage controls. Examples of policies that can be federated include users' permissions on the file, file owner, classification of a file and watermarking to be displayed on the file. The synchronization of policies between the application and Seclore Data-Centric Security ensures a streamlined and dynamic extension of file usage permissions.

Dynamic and Automatic Policy Management

A change in file permissions in the security software offering and business application will be automatically applied – in real-time – on all downloaded protected files for simplified administration.

Remote Control

The file owner can control the usage policies even after a protected file has been shared. All changes in usage permissions take effect in real time.

Online Editing-as-a-Service

Allows the business application to open and edit Seclore-protected files in a secure browser with a single click. Documents edited will be saved back to the business application.

Integrated Auditing

All activities performed on protected files – whether inside or outside the enterprise network - are centrally logged. Email alerts on unauthorized usage attempts (e.g. someone tried to print a protected file) can also be configured. SIEM tools like Splunk and BI Analytics tools can also be integrated with Seclore to provide centralized auditing and compliance reporting.

Seclore SDK Use Cases

Here is how various business and security software offerings can be extended with data-centric security to better address security, regulatory compliance and agility challenges:

Solutions	Sample Seclore Custom Integration Use Cases
Content Collaboration Platform (CCP)/Content Management Systems (CMS) + Seclore	**Use Case – 1:** Files downloaded or uploaded through CCP/CMS can be automatically protected by calling the Seclore SDK. The relevant Rights Management policy will be applied to the file which ensures efficient flow of information while removing the security risk.
Data Loss Prevention/CASB + Seclore	**Use Case – 2:** Sensitive data discovered by DLP on Endpoint, Network File Shares or data being uploaded to the web will be automatically protected by calling the Seclore SDK. The relevant Rights Management policy is applied to the file so that the file can be freely shared across and outside enterprise boundary. **Use Case – 3:** Sensitive data discovered by DLP in an email will be automatically protected by Seclore by adding a X-Header in the email. This X-Header will be read by a Seclore service to apply the relevant Rights Management policy. **Use Case – 4:** Detect and decrypt protected data to enable DLP to scan content before it exits enterprise boundaries via email or web traffic. This can be achieved by calling the Seclore SDK to allow the DLP solution to perform content inspection. **Use Case – 5:** Files downloaded or uploaded through sanctioned or unsanctioned CASB applications will be automatically protected by calling the Seclore SDK. The relevant Rights Management policy can be applied to the file so that it can be freely shared across and outside enterprise boundary.
Data Classification + Seclore	**Use Case – 6:** Sensitive documents or emails classified by a Data Classification system will automatically be protected by calling the Seclore SDK. Granular Rights Management usage controls are automatically applied to the file based on the classification label, giving the company on-going control over the document usage (cut/paste, print, etc.) and tracking.

Solutions	Sample Seclore Custom Integration Use Cases
Data Classification + Seclore (continued)	**Use Case – 7:** Sensitive emails classified by a Classification system will be automatically protected by Seclore by adding a X-Header in the email. This X-Header will be read by a Seclore service to apply the relevant Rights Management policy.
BI & Analytics Tools + Seclore	**Use Case – 8:** Reports downloaded or shared as emails will be automatically protected by calling the Seclore SDK. The relevant Rights Management policy is applied to the file so that sensitive reports remain secure while being utilized outside the application.
Transactional Systems (ERP/ CRM/HRM) + Seclore	**Use Case – 9:** Auto-generated and manually exported reports will be automatically protected by calling the Seclore SDK. **Use Case – 10:** Reports sent as email attachments will be automatically protected by Seclore either by adding a X-Header in the email or by calling the Seclore SDK. This X-Header will be read by a Seclore service to apply the relevant Rights Management policy.
Enterprise Mobility Management (EMM/MDM) + Seclore	**Use Case – 11:** Securely access and utilize protected emails and documents on MDM-enabled devices. Works with most MDM vendors including BlackBerry, IBM MaaS 360, MobileIron, AirWatch and more.

Key Benefits

Security Software Providers	Enterprises
Increase the Competitiveness of Your Security Software Offering Adding data-centric security to your offering will enable you to seamlessly extend your solution's security to wherever your customers' data travels, enabling you to stand out from the crowd and other single-vendor 'one-size-fits all' solutions.	**Increased Data Security** By automatically adding persistent, granular usage controls to your sensitive information as it leaves your enterprise applications, you will obtain the freedom to securely collaborate and share information with vendors, partners, and contractors. As well, you can confidently utilize innovative technologies including personal mobile devices, content collaboration platforms and cloud-based solutions.
Easily Add Automated Data-Centric Protection to Your Security Software Offering The configurable, open nature of the Seclore SDKs make it easy for you to extend the power of your solution to include persistent, granular usage controls and tracking of sensitive content.	**Increased ROI from Your Existing Investments** The ability to easily add data-centric security to your existing transactional and business systems will enable you to seamlessly extend your security to wherever your information travels during the collaboration process.
Secure External Collaboration - Solve Your Customer's Last Mile Challenge Integrating your offering with Seclore's data-centric security will empower your customers to better secure information, address regulatory compliance, and confidently embrace their cloud, BYOD and outsourcing strategies.	**Simplified Administration - Common Policy Management Framework** Seclore's Policy Federation capability eliminates the need for separate 'policy' management for the same information. A common usage control framework helps bring your data governance framework under one roof by providing a single source-of-truth for information access and usage policies.

Security Software Providers	Enterprises
Help Your Customers Better Address Regulatory Compliance The ability to protect and audit data wherever it travels enables your customers to automatically track the usage of information and better comply with regulatory obligations for the entire lifecycle of the data - both within and outside their enterprise network.	**End-to-End Auditing and Regulatory Compliance** You can now govern the use of your information throughout its entire lifecycle – both within and outside your enterprise boundary.
Deliver Thought-Leadership Combining the Seclore Data-Centric Security Platform with your offering will offer your customers a way to easily unify leading-edge, best-of-breed technologies to better address their security, compliance and agility challenges.	**Increased Business Agility** Leverage and unify your current and future best-of-breed DLP, CASB, Data Classification and Rights Management to automate and optimize your overall data security with the Seclore Data-Centric Security Platform

The Power of Data-Centric Security

By combing the power of best-of-breed Discovery systems (DLP, CASB), Data Classification, Data Repository systems (CCP, CMS, ERP), Identity and Access Management (IAM) Systems, BI and Analytics tools and Rights Management with existing enterprise systems, organizations will achieve unprecedented control and monitoring of their sensitive information assets wherever they travel, including while they are being utilized by end-users.. Unified data-centric security will enable organizations to reduce security breaches, readily engage in secure external collaboration, rapidly address regulatory compliance, and gain the confidence to fully embrace the cloud, BYOD and outsourcing.

Global Headquarters
USA – West Coast
691 S. Milpitas Blvd
Suite 217
Milpitas, CA 95035
1-844-473-2567

USA – East Coast
Graybar Building
420 Lexington
Avenue
Suite 300
New York, NY 10170

Europe
Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 7621 5500 350

India
Excom House Second Floor
Plot No. 2,
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072
+91 22 6130 4200
+91 22 6143 4800

Saudi Arabia
5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

Singapore
Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton Way
Level 34-01
Singapore – 068811
+65 8292 1930
+65 9180 2700

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City
PO Box 73030
Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

SECLORE