Stop Monitoring Your Data. Protect It with Skyhigh Cloud Access Security Broker (CASB) and Seclore Data-Centric Security:

Skyhigh Cloud Access Security Broker (CASB) and Seclore data-centric security ensure that your most sensitive data is discovered and protected— whether it travels across the cloud or to third-party business partners. Seclore's persistent security policies are automatically attached to documents when discovered, regardless of the file type.

Security permissions can be modified or revoked anytime, even after a file is downloaded and saved to a personal computer or offline media, like a USB. You can easily comply with data security regulations using data-centric tracking, and real-time alerts of unauthorized usage attempts.

The Business Problem

You've invested in discovering and monitoring your organizations sensitive information in the cloud repositories with a cloud access security broker (CASB) solution. However, what happens after data discovery?

- How are you protecting the sensitive data moving outside your network for external collaboration?
- Are you leveraging the full capabilities of your CASB solution?
- Are you concerned about the necessary resources to implement CASB and the SOC remediation team to maintain them?
- Do you find the deployment of CASB challenging—defining business rules, reviewing exceptions and false positives, testing, tweaking, and repeating rules?
- Once you've discovered sensitive information, how do you persistently control the document even while it is in use?

That is where Skyhigh and Seclore together can help.

Leverage the Combination of Skyhigh Security and Seclore to Stop Chasing Your Data

The combination of Seclore and Skyhigh CASB allows you to gain control over the use of your sensitive information—including the power to revoke access entirely—even when documents travel beyond the network perimeter. When Skyhigh CASB discovers sensitive data, Seclore automatically protects it with your pre-defined usage control policies. The granular usage controls stay with the file wherever the file travels or resides and protects the data while in transit (sent via email), at work (in use), and at rest (on any file format, device, or operating system).

Combining the Skyhigh Security CASB solution with Seclore data-centric security allows you to gain best-in-class technologies from two worldwide industry leaders. Only Seclore data-centric security combined with Skyhigh CASB delivers:

Automatically adding granular usage controls to files based on Skyhigh CASB discovery and actions.

Tracking usage of documents for simplified audit and compliance reporting.

Utilizing protected documents on any device, platform, and browser.

Revoking access to protected documents remotely.

Military-grade data-centric security tested by governments and defense agencies worldwide.

Advantages of Combining Seclore data-centric security with Skyhigh CASB

- Change your security posture from “reactive” to “proactive.”
- Protect your data as opposed to chasing your data.
- Secure data beyond the organization.
- Accelerate CASB deployments to increase time to value.
- Reduce false positives, administrative overhead, and SOC remediation efforts.
- Zero dependencies on users to classify or protect data.
- Dynamically assign and revoke granular usage permissions instantly.
- Add persistent data-centric security, controlling who does what, when, and from where
- Gather forensic detail on data usage, ensuring you meet regulatory and privacy compliance.

Shifting to a Proactive Security Posture by Adding Data-Centric Security

Seclore data-centric security changes your security posture from “reactive” to “proactive” when using a CASB solution. “Monitor Mode” is a standard deployment of CASB providing dashboards, reports, and alerts; however, the security concern is that once sensitive data leaves the enterprise, you’ve lost control and visibility of your data. With Seclore, you can automatically add access and usage controls to “discovered” data (email and cloud) before data leaves your enterprise so your employees and third parties can continue working and collaborating securely. Shifting your security strategy from detecting, monitoring, and chasing your sensitive data to automatically securing your discovered data before sending it allows you to control your sensitive data.

Additionally, Seclore data-centric security accelerates your CASB deployments by becoming the ‘default’ business rule—protect all sensitive data discovered and shared outside the organization. Adding data protection to CASB eliminates ongoing configuration changes and endless testing cycles required to create business rules, which are not too stringent or lenient. The by-product of protecting discovered data is a significant reduction in security operations center (SOC) remediation efforts related to exception handling of “false positives,” saving valuable time and costly administrative overhead.

The combination of CASB and Rights Management ensures:

Zero User Intervention

Automation across the discovery, protection, and tracking process to consistently close security gaps with zero user intervention.

Deployment Costs

Reduction in deployment costs while increasing your “time to value” of the combined offerings.

Leveraging Existing Enterprise

Confidence in leveraging existing enterprise systems (Email, Content Collaboration, Business Applications) across all business processes.

Tangible Return on Investment (ROI)

SOC remediation efforts dramatically decrease while business workflows continue uninterrupted, providing a tangible return on investment (ROI).

Seclore data-centric security and Skyhigh Security Cloud Protection

Skyhigh Security and Seclore provide automated file protection in the cloud. When users save or move files into cloud-based applications like Box, Teams, SharePoint, or OneDrive, Skyhigh Security scans and discovers the files. If the files contain sensitive information, Seclore automatically protects them.

Figure 1. How Skyhigh Security and Seclore work together to protect sensitive data within Cloud applications

Seclore Automatic Email Protection and Skyhigh Security Email Cloud

Seclore offers a secure and streamlined solution that addresses the most common method of collaboration— email. Once Skyhigh Security discovers emails, any email containing sensitive content is tagged. Seclore automatically protects all sensitive emails which have been tagged by Skyhigh security. With Seclore automated email protection, data sharing can continue seamlessly while still maintaining security and compliance. This protection is entirely transparent to the email sender and recipient.

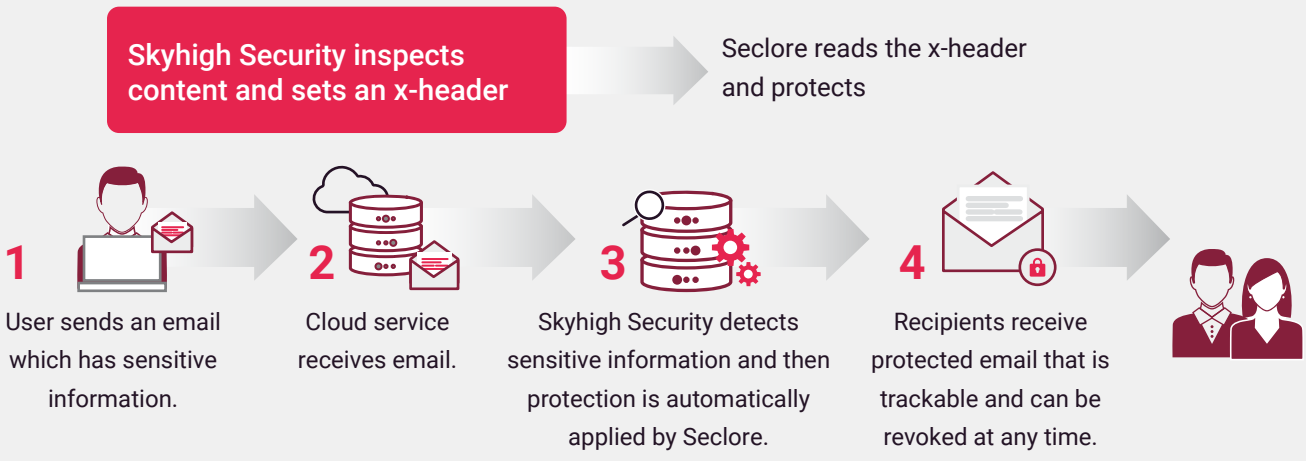


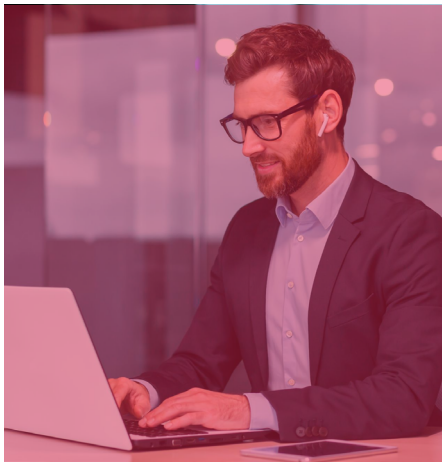
Figure 2. How Skyhigh Security and Seclore work together to protect sensitive data shared via email.

Skyhigh Security and Seclore: The Complete Data-Centric Security Solution

Combining Skyhigh Security CASB with Seclore data-centric security will give you unprecedented control over sensitive information—with content-aware, boundary-independent, and entirely automated security. Seclore also allows you to reap the full benefits of Skyhigh Security and extend its jurisdiction to external collaborators, the cloud, and mobile devices.

Skyhigh Security-compatible solutions integrate with the following:

- Seclore Data-Centric security
- Seclore Email Encryption Plus



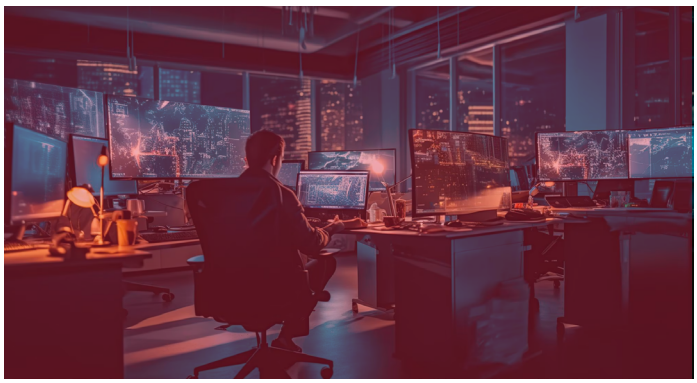
About Seclore

Offering the market's first browser-based solution, the Seclore data-centric security Platform gives organizations the agility to utilize best-of-breed solutions to discover, identify, protect, and track data usage.

The Seclore data-centric security platform is the most advanced, secure, and connected to industry leaders such as Skyhigh Security, protecting sensitive files in transit, at rest, and even in use. Over 2,000 customers in 29 countries use Seclore to achieve their data security, governance, and compliance objectives.

About Skyhigh CASB

Skyhigh CASB protects data from device to cloud and prevents cloud-native threats that are invisible to the corporate network. This creates a secure environment for adopting cloud services, enabling access from any device and ensuring workforce productivity.



SECLORE™

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.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054