

# Large U.S.-Based Financial Services Firm Strengthens User Governance with Intralinks SecurityHub Pro

A large U.S.-based financial services firm has been a long-standing Intralinks customer and is one of the largest wealth management and investment banking institutions in the country. The firm's mergers and acquisitions (M&A) team has relied on Intralinks for years for traditional deal activities.

In 2023, the firm sought to enhance access security by implementing single sign-on (SSO). Their goal was to tighten access controls and prevent bankers from retrieving legacy deal data from prior projects. What began as a request to streamline authentication expanded into a broader conversation about governance and compliance. This collaboration ultimately led to a successful upgrade to [SecurityHub Pro](#) powered by Identity+.

## Problem

Before implementing SSO, the firm's IT team identified a major compliance challenge: a significant number of users were still accessing multiple Intralinks data rooms using shared group email addresses. This practice, particularly prevalent in the wealth management division – one of the heaviest users of Intralinks – made it nearly impossible to track who was logging in, what they were accessing and whether they were still authorized.

Removing group emails entirely wasn't a viable option, as the firm estimated that the re-onboarding process could take six months to a year, introducing significant disruption and delays. The IT team needed a solution that maintained the functionality of group email access while enabling them to maintain compliance and oversight effectively.

## Client Success Story

U.S.-Based Financial Services Firm



**Industry:**

Banking & Wealth Management



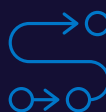
### Improved security posture

Stopped unauthorized access via group email addresses



### Comprehensive visibility

Gained granular, real-time user access insights



### Seamless implementation

Maintained existing workflows while bolstering security controls

## Solution

During the SSO implementation, the firm’s IT team uncovered the challenges posed by shared group email access and partnered with Intralinks to develop a more advanced solution. This collaboration involved in-depth technical discussions across multiple teams, including product experts, service delivery, and the wealth management and compliance stakeholders.

The breakthrough came with [SecurityHub Pro](#) featuring Identity+ – a purpose-built feature that balances flexibility with control. Identity+ allows users to continue logging in through shared inboxes while providing the IT department with full visibility into individual user activity across Intralinks data rooms. This ensures the wealth management, investment banking and debt capital markets teams can maintain existing workflows without compromising security or compliance.

## Results

By implementing [SecurityHub Pro](#) with Identity+, the firm preserved its group email workflows while gaining audit-level visibility into user activity. This avoided a disruptive overhaul that would have required re-inviting individuals to more than 77 data rooms, a process that could have taken six months to a year to complete. With real-time access logs and an intuitive dashboard, the IT team can now easily identify users, monitor usage and remove access when needed.

This enhanced transparency empowered the firm to enforce compliance policies more consistently and proactively manage risk. What began as a straightforward SSO request evolved into a scalable initiative that significantly elevated the firm’s security posture. The solution not only met the firm’s immediate goals, it also saved months of manual work, surfaced new governance opportunities and strengthened user management practices across the enterprise.

