SplitSecure

**Tristan Morris**
Cofounder & CEO
tristan@splitsecure.com

# A Simple and Effective Tool for Managing Third-Party Risk

SplitSecure gives financial institutions simple, direct control over third-party risk—without heavy tools or cumbersome audits.

REGULATORY REALITY

## Financial institutions face increasing scrutiny

Financial institutions face increasing scrutiny from regulators on how they manage their third party risk. The recent vendor breach that exposed hundreds of community banks demonstrates the dangers: third parties hold persistent access and credentials banks cannot control or monitor.

The **New York Department of Financial Services** (NYDFS) recently issued guidance on third-party vendor risk management to the financial institutions it covers.

**NYDFS** now requires banks to validate:

- Auditing
- Monitoring
- Drift detection
- Integration risk
- Control changes

Validation must be based on observable results—not self-reported controls.

## ⚠ The Problem

Regulators emphasize that third-party relationships reduce a bank's direct operational control.

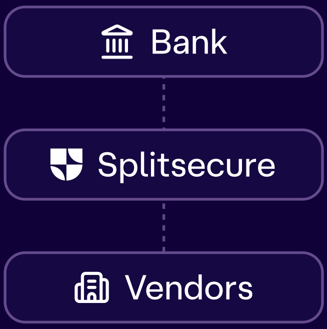
## ☑ The Solution

SplitSecure restores that control by placing all vendor access behind a provable, bank-owned approval layer.

SPLITSECURE MODEL

## A bank-owned access layer

SplitSecure offers a new, dramatically simpler way for financial institutions to manage third-party cybersecurity risk. SplitSecure gives every financial institution, large or small, the same advanced access-control protections used by top-tier security teams, without requiring new headcount or complex integration.


Bank

Splitsecure

Vendors

**SplitSecure** is an **access control platform**, which can be deployed as a middle layer between the financial institution and their third-party vendors.

HOW IT WORKS

## With SplitSecure...

### No third party ever has access

Access to credentials, keys, or other secrets is always ephemeral and fully controlled by the financial institution.

### Guaranteed audit logging

Every access event is mathematically guaranteed to be audit logged, meeting all NYDFS validation requirements and creating a “single source of truth” for automated processes.

### Single enforcement platform

Vendor access to systems, accounts, and data is centrally managed—manually or through automated policies—allowing SplitSecure to serve as the institution’s unified enforcement layer.

CRYPTOGRAPHIC ASSURANCE

## No added third-party risk

Unlike other vendors, SplitSecure never has access to the information it protects. Everything is controlled by the financial institution, so we never add to your third party risk. Our technology is based on a cryptographic technique called Shamir Secret Sharing, previously used by the NSA, Brex, and Google for protecting their most sensitive organizational secrets.

THE FOUNDERS

## Built by leaders in security engineering.

**Tristan Morris**
Cofounder & CEO

Tristan Morris is a security engineering prodigy who started attending college at age 12. After graduating from Cornell, he went on to lead Federal Security at KNOX, Samsung’s military and defense cybersecurity group.

**Marc Trembley**
Cofounder & CTO

Marc Tremblay has been a security engineer on some of the most capable and prestigious security teams in the world, including the core security teams of Netflix and Stripe. He has six patents for security technology.

## Ready to regain provable control over third-party access and vendor risk?

Email us directly at **tristan@splitsecure.com**