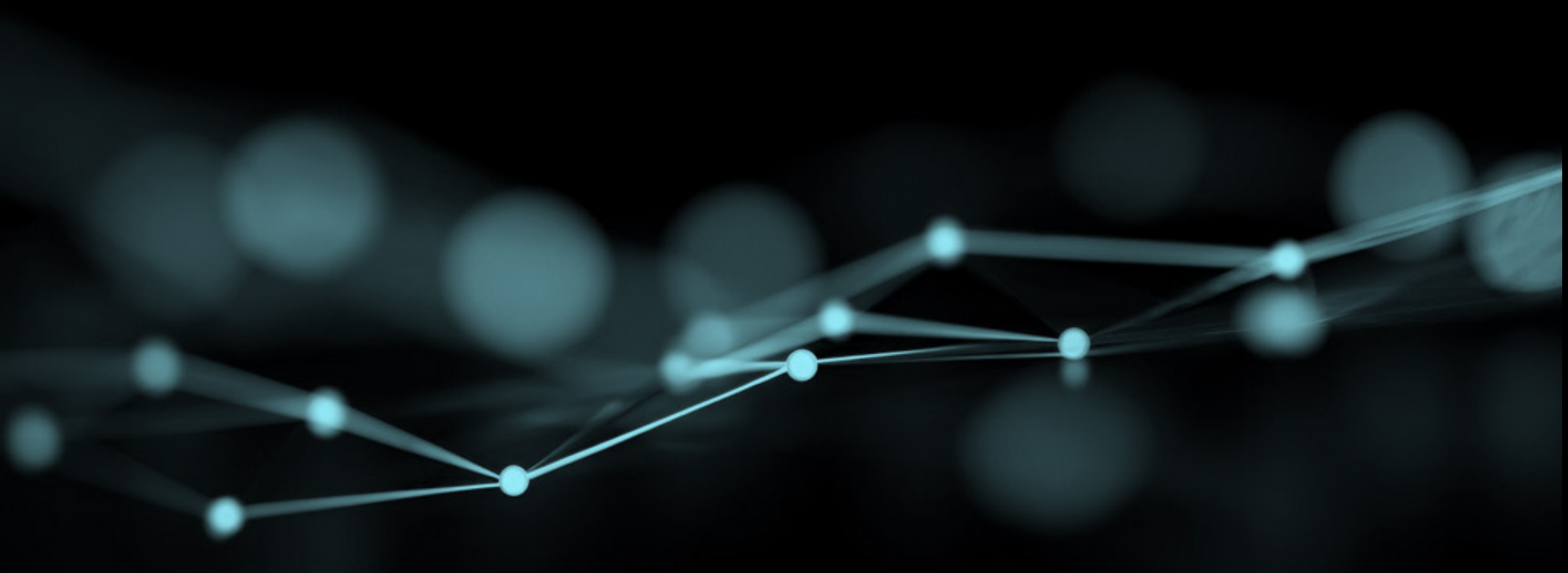
Rhino
Federated Computing

AML & FinCrime Tech Forum

PRESENTATION INSIGHTS

From Siloed Signals to Collaborative Crime Fighting with Federated Computing

Chris Laws, Chief Commercial Officer



Introduction

Financial crime is a growing challenge, with sophisticated criminal networks exploiting blind spots in isolated systems. Even the largest financial institutions struggle to see the full picture, leaving gaps that criminals can easily exploit.

Enter Federated Computing, a groundbreaking approach that enables collaboration without compromising data privacy or security.

Rhino
Federated Computing

The Problem: Fighting Financial Crime in Isolation

Traditional methods of combating financial crime are limited by:

Data Silos: Institutions only see their own data, missing the broader criminal network.

Privacy Regulations: Sharing raw data is restricted by laws and security concerns.

False Positives: Isolated systems often flag legitimate transactions as suspicious, wasting resources.

Rhino
Federated Computing

The Solution: Federated Computing

Federated Computing allows institutions to **collaborate by sharing insights, not data**.

This approach combines Edge Computing, Federated Learning, and Privacy-Enhancing Technologies to **create a secure, decentralized network for fighting financial crime**.

Rhino
Federated Computing

How Federated Computing Works

1. **Local Training:** Each institution trains models on its own data.
2. **Global Aggregation:** Insights are shared and aggregated without moving raw data.
3. **Local Deployment:** Institutions use the global model to detect patterns and anomalies.

Rhino
Federated Computing

Use Cases in Financial Crime Prevention

- **Fraud Detection:** Banks share "fraud signals" instead of raw data, doubling detection accuracy and reducing false positives.
- **KYC/KYB:** A Federated Verification Layer speeds up onboarding by learning from decentralized networks.
- **Mule Account Sharing:** Real-time identification of suspicious accounts stops money laundering in its tracks.

Rhino
Federated Computing

Real-World Examples

Project Aikya: J.P. Morgan and BNY Mellon proved that federated learning can identify payment anomalies faster than isolated systems.

Project Aurora: BIS Innovation Hub uses privacy-enhancing technologies to combat money laundering across borders.

Project COSMIC: Singapore's MAS enables secure sharing of customer information to fight global money laundering.

Secure Data Collaboration: Swift is piloting the use of Federated Analytics for sharing information on mule accounts and Federated Learning for predicting fraud.

Rhino
Federated Computing

The Future of Federated Computing

While financial services are still exploring proofs of concept, other industries like biopharma are already leveraging federated computing for production workloads. The potential for financial crime prevention is immense, but institutions must act now to stay ahead.

Rhino
Federated Computing

Don't let your AI strategy operate in isolation. Join the federated future by:

- Participating in collaborative initiatives like Swift or BIS.
- Building a consortium with peers to pilot federated solutions.
- Upgrading infrastructure with partners like NVIDIA and Rhino Federated Computing.

Rhino
Federated Computing

Contact us to view a demo

As Boston Consulting Group aptly puts it:

"If you want to be incrementally better: Be competitive. If you want to be exponentially better: Be cooperative."

contact@rhinofcp.com

www.rhinofcp.com

Rhino
Federated Computing