SECLORE™

Secure Collaboration in the BFSI Sector – The ASEAN Chapter

Banking Without Borders, Safely

Book a Demo

Introduction: The New Reality of Digital Collaboration in ASEAN Banking

Digital transformation is reshaping how ASEAN banks communicate, share, and store sensitive data. From credit scores and KYC files to customer PII, data now moves through complex networks of fintechs, vendors, and regulators.

Once data leaves the bank's perimeter, traditional controls like firewalls, encryption, and DLP can't guarantee security.

ASEAN digital economy by 2030

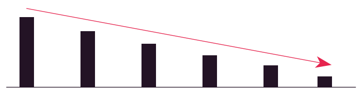
US $300 Bn → US $1 Tn

Growth on a trillion-dollar scale

Banking as a major component

[WE Forum]

80% of digital organisations will fail



Because they don't adopt a modern approach to data governance

Modern data governance = business survival

[Gartner]

Banking Technology is Spending in APAC (2022 - 2023)

$63B	$68B
2022	2023

Focus shift to cloud, AI & ML

[ASEAN Banks: 10x]

Vietnam's Digital Usage

55%	2017
88%	2021

Digital growth on the rise

[ASEAN Banks: 10x]

Data Exposure Risk in Financial Services Sector

Total Sensitive Files	Files Exposed
449,855	36,004

Varonis

Once data leaves the bank's systems, visibility and control drop sharply — each shared dataset becomes a new endpoint of risk.

ASEAN Stats: Country-Specific Stats

Vietnam's Digital Banking

87% of adults now have bank accounts

95%+ of transactions happen digitally

Vietnam leads Southeast Asia in digital banking growth

[Vietnam Plus]

Malaysia's Shift to the Cloud

2022

5 Digital Bank Licenses Issued

Transforming banking through digital innovation

From Banks to Cloud

2025

95% Cloud-Ready by 2025

[Fintech News]

The Collaboration Imperative in Modern BFSI

Collaboration drives competitiveness. Banks that fail to modernize secure data-sharing risk compliance penalties and lost agility.

Global Cost of Data Breaches Drops

USD 4.44 Million

-9% from last year

[Cost of Data Breach 2025: IBM]

Data Breach Lifecycle Shrinks

2024: 258 days
Slower breach response

2025: 241 days
Faster containment

17 days faster to identify and contain breaches

[Cost of Data Breach 2025: IBM]

Nearly Half of Financial Firms Hit by Breaches

46%

Data breached in past 24 months

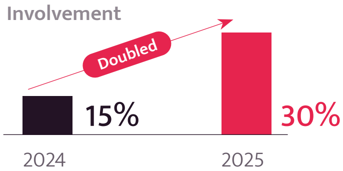
[Helpnet Security]

Information Loss Drives Cyber Costs

43% of breach costs come from information loss

[Cost of Data Breach 2025: IBM]

Data Breach Doubled with Third-Party Involvement



[Verizon DBIR 2025]

Identity Gaps in Access Security

Lack of identity security solutions for non employees

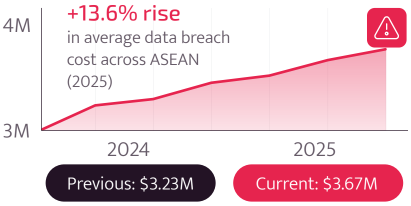
47% desired to address the gap

[Helpnet Security]

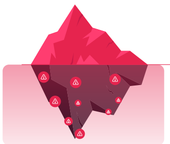
Security Risks in the Collaboration Environment

As digital connections multiply, new attack vectors emerge — from phishing and insider misuse to exposed vendor systems.

Rising Data Breach Costs in ASEAN



Vulnerabilities Across in Southeast Asia's Banks



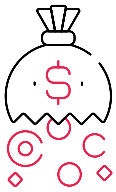
Study Across 90 financial services organizations

Visible Security

26,500+ Hidden Vulnerabilities

[TechRepublic]

ASEAN Finance Breach Costs Surge



$5.56M Average cost per data breach (2025)

[Cost of Data Breach 2025]

Top Cyber Threats in 2025

- Ransomware
- Supply Chain Breaches
- AI-Driven Fraud
- Phishing Attacks

Finance Sector: The Prime Cyber Target

300× More cyberattacks than any other industry.

[KnowBe4 2025]

Origins of Financial Breaches

- **78%** External
- **22%** Internal
- **1%** Partners

[Verizon DBIR 2025]

AI Adds a New Edge to Cybercrime

16% of breaches involve AI

Shadow AI drives up cost & breach time

[Cost of Data Breach 2025]

Third-Party Access: A Growing Concern

Too Much Access

80% worry about risks from excess third-party non-employee access

[Helpnet Security]

Where ASEAN Banks Lose Control – And How to Gain It

Once sensitive data leaves internal systems — through vendor collaboration, outsourcing, or cross-border sharing — banks lose visibility and control. Traditional defenses like firewalls and DLP stop at the perimeter. This is where data-centric security takes over — embedding protection within the file itself.

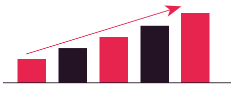
Seclore enables **data-centric security** that travels with the file — across emails, cloud drives, or shared portals.

- Automatically **classify** and **encrypt** sensitive documents (PII, KYC, risk reports).
- Apply **usage controls** — restrict viewing, forwarding, or printing.
- **Track** and **revoke access** even after files are shared externally.
- **Integrate** with existing platforms (M365, Salesforce, AWS, Azure, Box).
- Provide real-time audit trails for **MAS TRM, BNM RMiT,** and **PDPA** compliance.

Building Secure Collaboration Frameworks

Leading ASEAN banks apply zero-trust architectures and granular control policies to ensure external collaboration remains compliant and auditable.

Secure Collaboration on the Rise



+25% YoY growth in secure collaboration platform adoption across **ASEAN** financial services (2025–2026)

ASEAN's Expanding Digital Bank Network

25+ digital banks now power ASEAN's modern finance network - building stronger regional links

[Statista / ASEAN Bankers]

The Payoff: Trust, Efficiency, and Growth

Purpose: Quantify benefits — security as a growth driver.

Secure collaboration is more than compliance; it enhances agility and customer confidence.

Faster Decisions with Secure Tools

30% faster decision-making through **centralized secure collaboration**

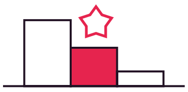
Lower Compliance Audit Costs

25% cost reduction with secure systems

Security Shapes Trust

87% of customers won't trust banks with weak data security (McKinsey 2025)

Finance Sector Among Most Breached



#2 worldwide for cyber breaches in 2022 - **financial sector** remains a top target

[American Banker]

Record Fines, Rising Stakes

amazon	€746M (2025)
DiDi	$1.19B (2022)
MARRIOTT	£18.4M (2020)
EQUIFAX	$575M–$700M (2019)

[American Banker]

Collaborate Securely. Compete Strongly.

As ASEAN's financial sector becomes increasingly connected and secure, external collaboration will define the region's next era of banking resilience and innovation.