MAY 5, 2022

FIGHTING DIGITAL FRAUD WITH CONFIDENTIAL COMPUTING

FIVERITY intel Fortanix

FIVERITY

Defense Against Digital Fraud

FOUNDED IN 2015

MULTIPLE INDUSTRY AWARDS

FDITECH
Measuring the Effectiveness of Digital Identity Proofing for Digital Financial Services

CYBER SECURITY
EXCELLENCE AWARDS
★ WINNER ★
2022

2022
GLOBEE AWARDS SILVER WINNER
CYBER SECURITY GLOBAL EXCELLENCE

BANKING TECH AWARDS USA | FINTECH FUTURES
Finalist

- Appointed by the **Federal Reserve Bank** to join the Synthetic Identity Fraud Focus Group to create a formal definition for synthetic identity fraud in 2020
- Selected as a winner by the **FDIC** and **FinCEN** in the 2022 FDITECH Sprint for the "Effectiveness/Impact" of its proposed solution, which leveraged Confidential Computing to validate remote digital identities

info@fiverity.com | fiverity.com

Fortanix®

FOUNDED IN 2016
Ambuj Kumar, CEO & Co-founder
Anand Kashyap, CTO & Co-founder

MULTIPLE INDUSTRY AWARDS
RSA Innovation Sandbox runner-up
Gartner Cool Vendor

cyber secured. AWARDS 2021

RSAC Innovation Sandbox 2018 RUNNER-UP

Cloud Computing 2019

Gartner Cool Vendor 2018

THE CHANNEL CO. CRN WOMEN of the Channel 2019

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2020

START-UP OF THE YEAR 2018

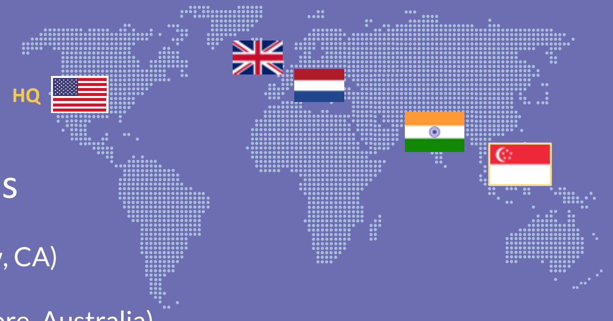
100+

Customers

intel. Standard Chartered PayPal adidas NEC UCSF Valeo

200

Employees in
5 Regional Hubs



- USA (Mountain View, CA)
- EMEA (Eindhoven)
- APAC (India, Singapore, Australia)

Series B (2019) Notable Investors

intel Capital iqt IN-Q-TEL foundation capital NEOTRIBE

25+ Patents granted/pending

Security at Scale

The scale of Intel’s security capabilities is unmatched.

500+
Dedicated product security staff

987
PSIRT tickets closed in 2020

7000
Active projects tracked in Intel’s Security Development Lifecycle system

400
Max. security tasks per project

IN 2020:

116
Public security whitepapers

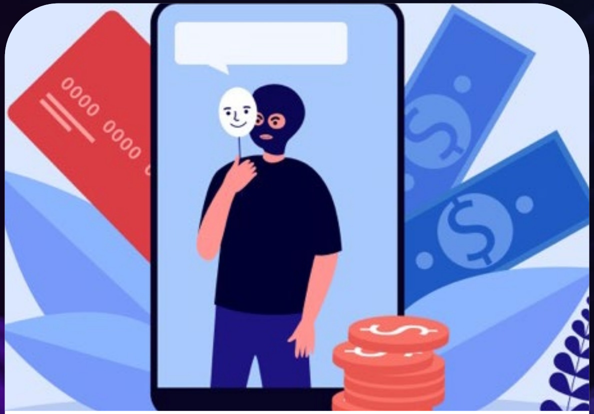
120
Hackathons held

40+
Academic research teams funded

Digital Fraud: Fastest Growing Threat

1.5 BILLION

PII ELEMENTS EXPOSED IN PAST 3 YEARS ALONE



UP TO HALF

OF NEW ACCOUNTS ARE FRAUDULENT

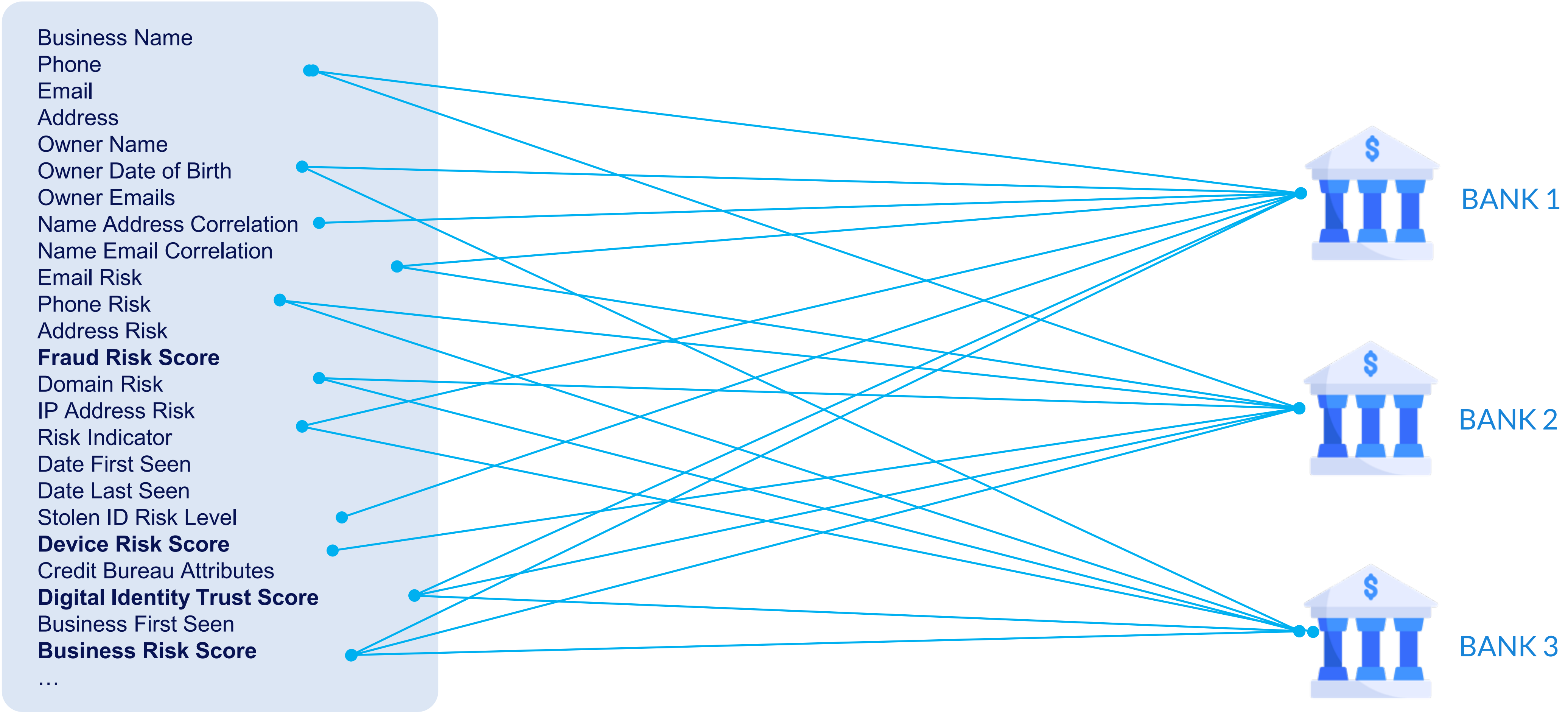
$52 BILLION

IN LOSSES FROM ID THEFT IN 2021

FDIC and FinCEN TechSprint: Digital identity proofing

> What is a **scalable, cost–efficient, risk–based solution** to measure the effectiveness of digital identity proofing to ensure that individuals who remotely (i.e., not in person) present themselves for financial activities are who they claim to be?

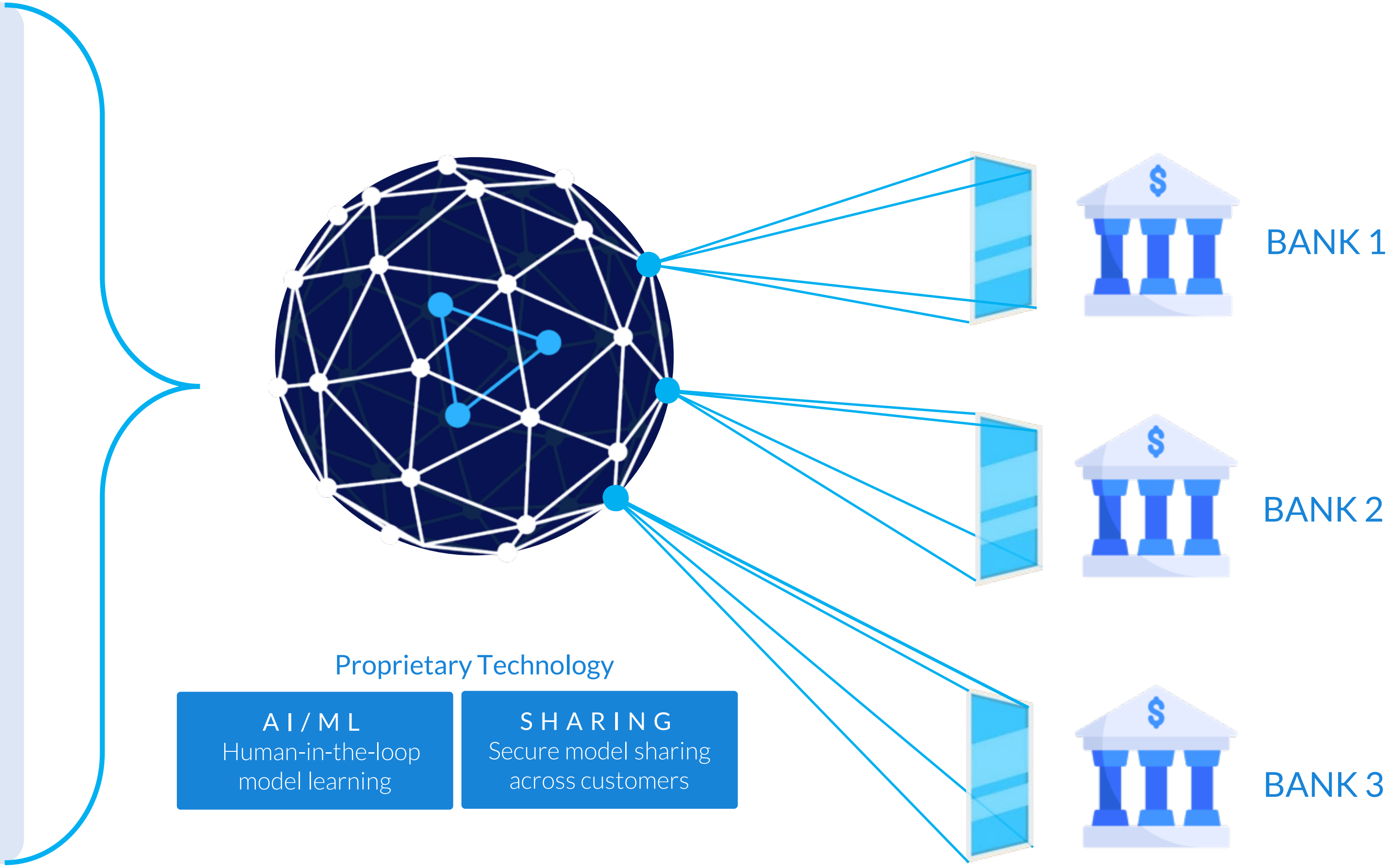
Current State of Fraud Data



Business Name
Phone
Email
Address
Owner Name
Owner Date of Birth
Owner Emails
Name Address Correlation
Name Email Correlation
Email Risk
Phone Risk
Address Risk
Fraud Risk Score
Domain Risk
IP Address Risk
Risk Indicator
Date First Seen
Date Last Seen
Stolen ID Risk Level
Device Risk Score
Credit Bureau Attributes
Digital Identity Trust Score
Business First Seen
Business Risk Score
…

Holistic View: Single Pane of Glass

Business Name
Phone
Email
Address
Owner Name
Owner Date of Birth
Owner Emails
Name Address Correlation
Name Email Correlation
Email Risk
Phone Risk
Address Risk
Fraud Risk Score
Domain Risk
IP Address Risk
Risk Indicator
Date First Seen
Date Last Seen
Stolen ID Risk Level
Device Risk Score
Credit Bureau Attributes
Digital Identity Trust Score
Business First Seen
Business Risk Score
…

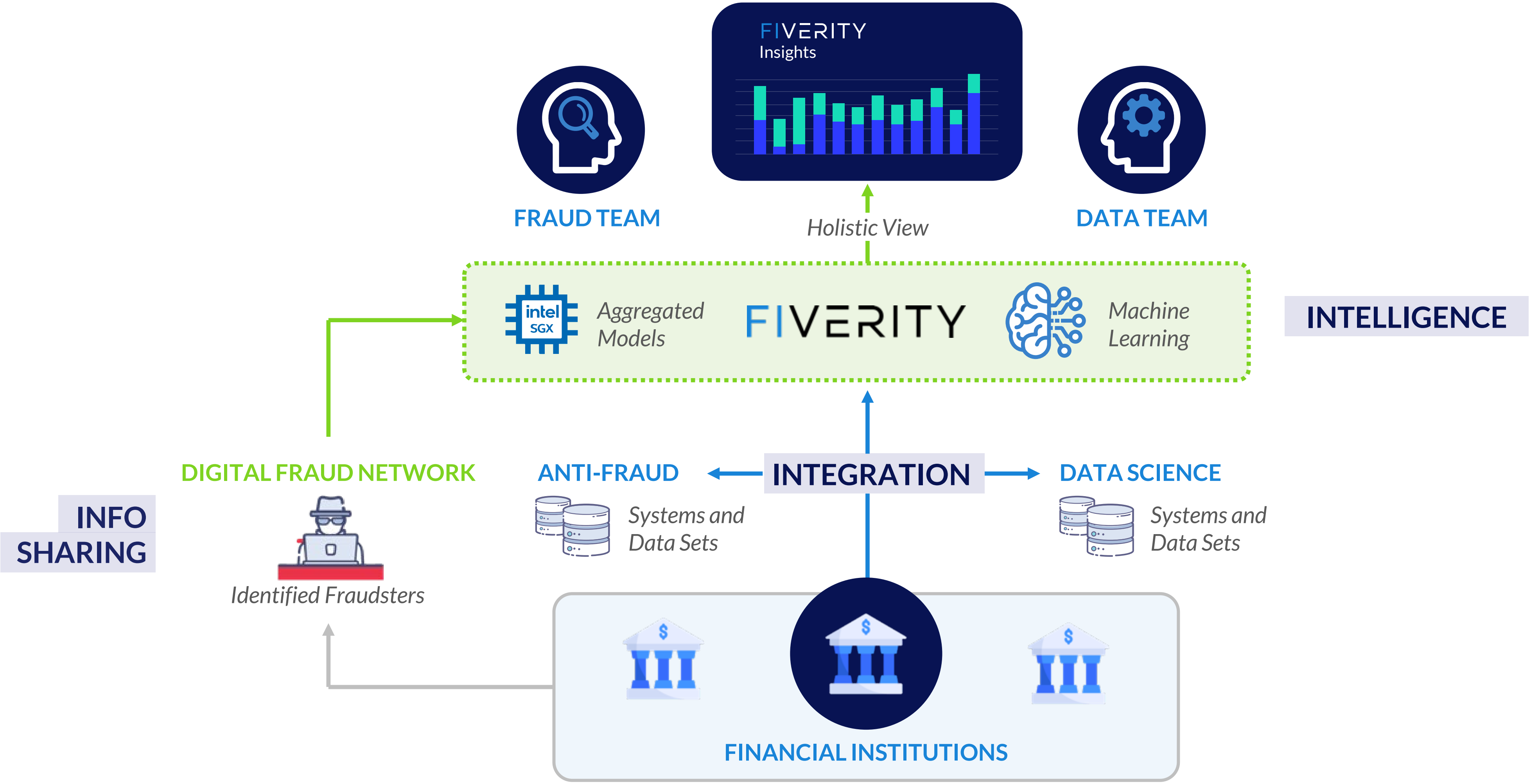


Proprietary Technology

AI/ML
Human-in-the-loop model learning

SHARING
Secure model sharing across customers

Holistic Platform: Digital Identity Proofing



FIVERITY Insights

FRAUD TEAM

Holistic View

DATA TEAM

intel SGX Aggregated Models

FIVERITY

Machine Learning

INTELLIGENCE

DIGITAL FRAUD NETWORK

Identified Fraudsters

INFO SHARING

ANTI-FRAUD

Systems and Data Sets

INTEGRATION

DATA SCIENCE

Systems and Data Sets

FINANCIAL INSTITUTIONS

How to Protect Data Privacy?

Business Name
Phone
Email
Address
Owner Name
Owner Date of Birth
Owner Emails
Name Address Correlation
Name Email Correlation
Email Risk
Phone Risk
Address Risk
Fraud Risk Score
Domain Risk
IP Address Risk
Risk Indicator
Date First Seen
Date Last Seen
Stolen ID Risk Level
Device Risk Score
Credit Bureau Attributes
Digital Identity Trust Score
Business First Seen
Business Risk Score
…

Need to obfuscate personally identifiable information (PII), while still collaborating with others and sharing threat information

Confidential Computing

- Safeguards PII in use
- Enables swift, secure growth

What are the threats to your data?

Hackers
Malware to exploit vulnerabilities in the hypervisor or OS

Malicious insiders
Those with escalated admin privileges

Third parties
Competitors or those who stand to gain by accessing data without consent

Data must be protected everywhere

At rest
Ensure data is encrypted when stored.

In flight
Ensure data is encrypted when transmitted.

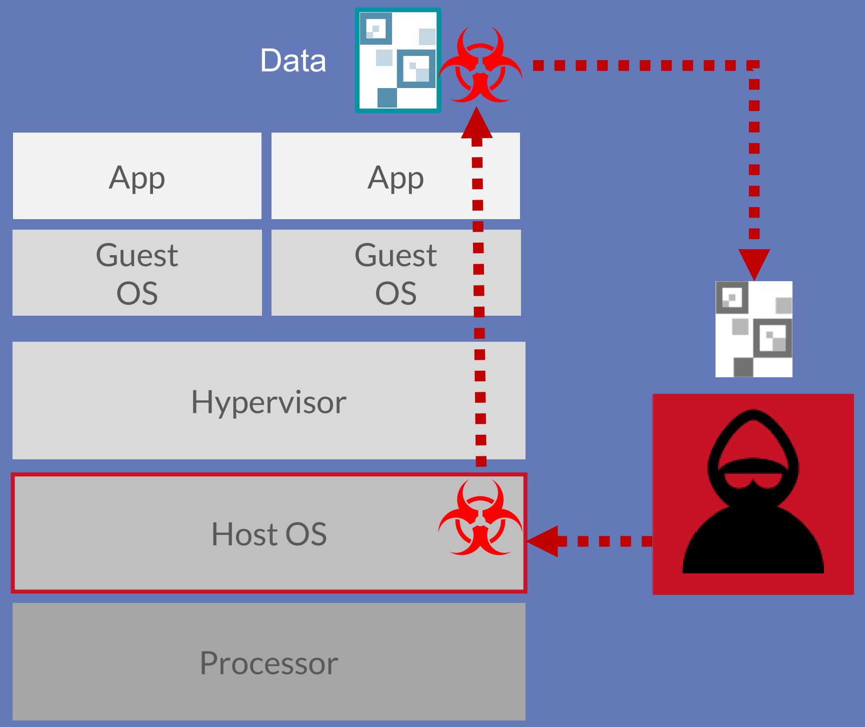
In use
This has been the most challenging gap for securing sensitive data—when it is decrypted and exposed in system memory during active processing.

Closing the in-use vulnerability is essential to maintain data privacy and security.

Why data remain vulnerable during active processing

ANATOMY OF A PRIVILEGE-LEVEL ATTACK

Traditionally, when a system's BIOS, hypervisor or OS have been compromised by a malicious attack, the attacker's code can gain visibility and access to applications and data residing higher in the system stack.

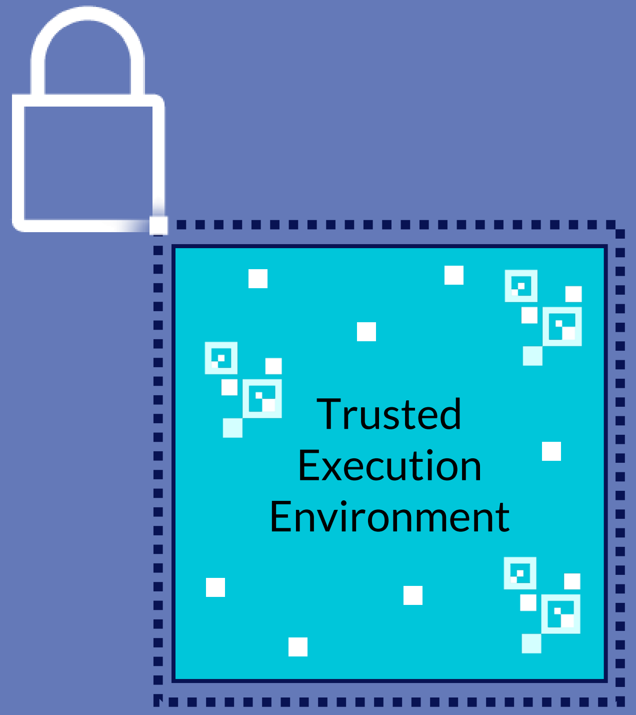


Without Confidential Computing

The Answer:
Confidential Computing

PROTECT DATA IN-USE

Confidential computing uses hardware-enhanced protection to create Trusted Execution Environments (TEEs) to isolate and protect data during active processing. There are varying ways to do these, each differing by how the protection is implemented and the size of trust boundary and attack surface remaining.

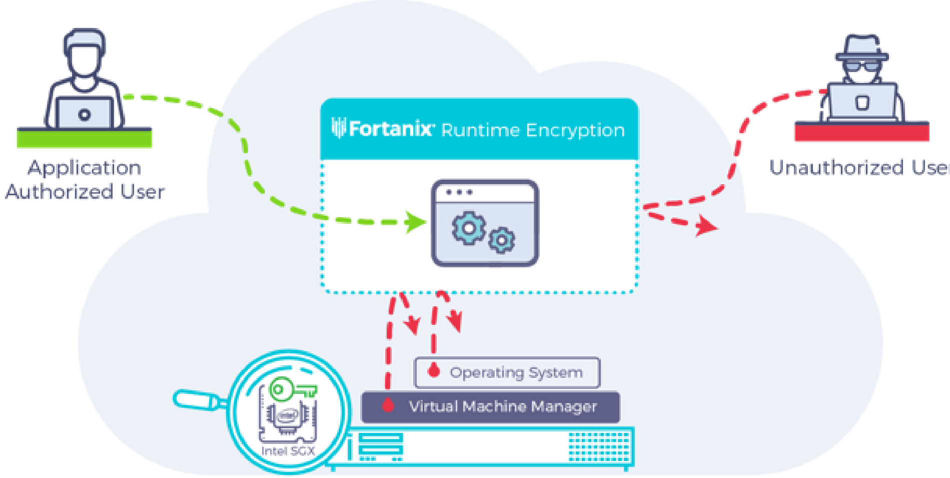


Confidential Computing

CONFIDENTIAL COMPUTING CONSORTIUM
GENERAL MEMBER

Confidential Computing

- Intel® Software Guard Extensions (Intel® SGX) uses hardware-aided security to provide a Trusted Execution Environment (TEE)
- Comprises a secure "enclave" where data and code are protected, even on an untrusted or compromised computing platform



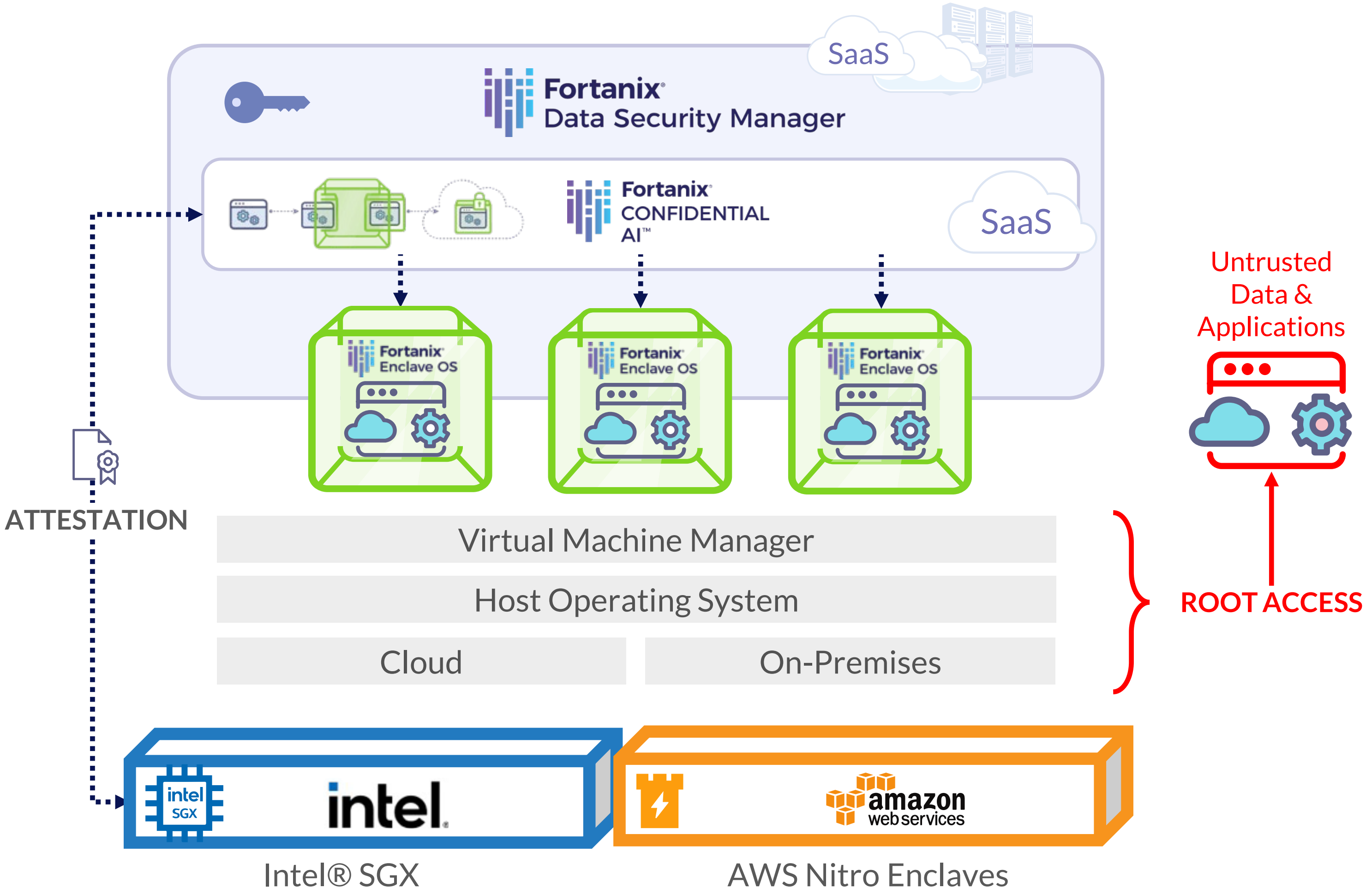
CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Computing Deep Dive v1.0

A Publication of The Confidential Computing Consortium
October 2020

https://confidentialcomputing.io/white-papers/

Confidential AI Stack



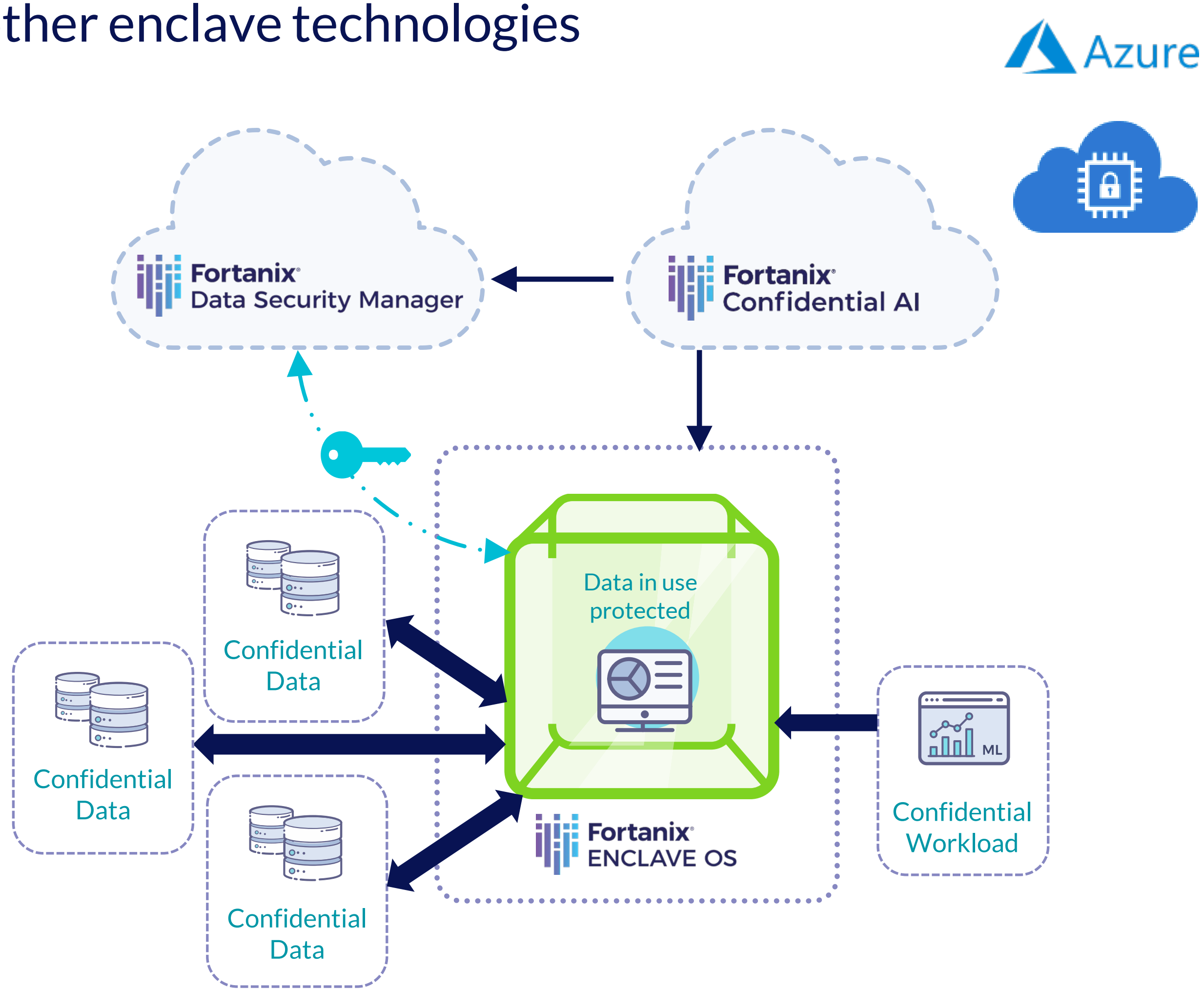
Fortanix Confidential AI

CUSTOMER USE CASES:

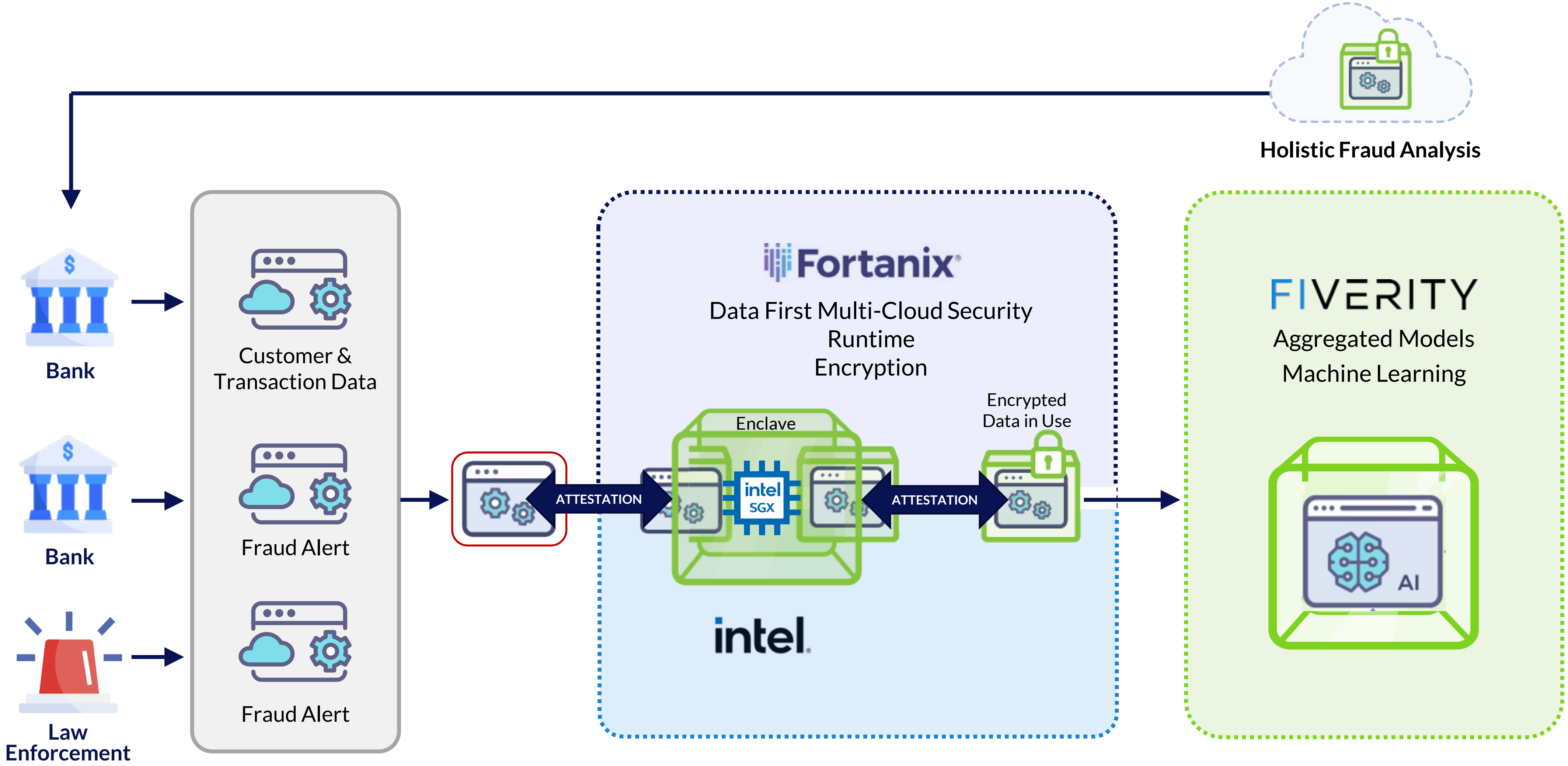
- Multi-Party Analytics
- Anonymous Data Sharing
- Anti-Money Laundering
- Identity Fraud Detection
- Genomics and Biopharma
- AI in Hospitals
- X-Ray and Scan Image Detection
- Secure Speech to Text

Securely run AI and ML models inside Intel SGX

and other enclave technologies



Identity Fraud Detection and Prevention Solution



Want to learn more? Visit fiverity.com/confidential-computing

Download the eBook: *Fighting Digital Fraud with Confidential Computing*

GREG WOOLF

CEO | FiVerity

gwoolf@fiverity.com

PATRICK CONTE

VP, Business Development | Fortanix

patrick.conte@fortanix.com

BRUNO DOMINGUES

CTO, Financial Services Industry | Intel

bruno.domingues@intel.com

THANK YOU FOR JOINING!

FIVERITY intel Fortanix