FIVERITY + intel + Fortanix

EBOOK

Fighting Digital Fraud with Confidential Computing

Confident Growth via Secure Fraud Management

Table of Contents

Introduction

While the adoption of Confidential Computing has the potential to transform many aspects of the financial services industry, its largest impact will be on digital fraud detection and prevention. By fully protecting sensitive data, Confidential Computing provides access to advanced fraud detection models that allow financial institutions to focus on acquiring legitimate customers.

In this eBook, we'll explore how Confidential Computing provides secure access to new tools to verify the identities of new and existing customers. We'll also review how Confidential Computing resolves data privacy and competitive concerns that have held back information sharing, which is proven to be a highly effective form of fraud detection.

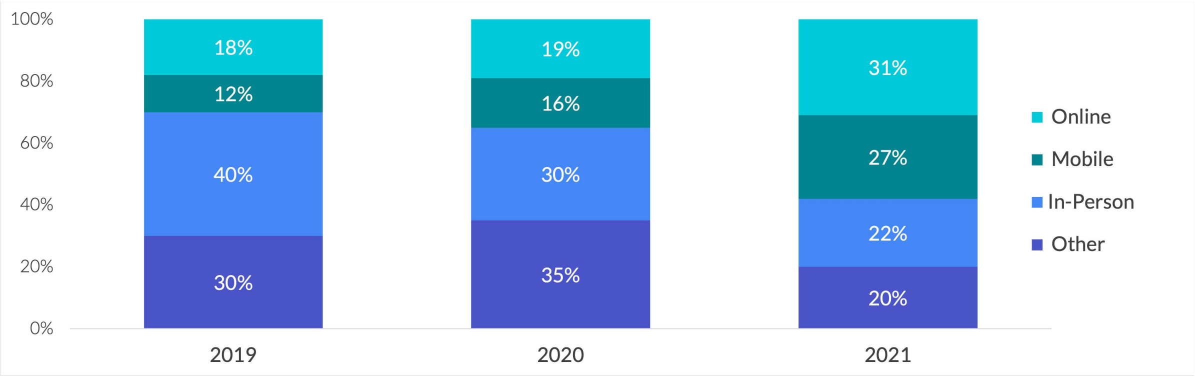
Confidential Computing Use Cases

Financial Services:	Healthcare:
• Aggregated fraud detection models • Crypto and digital asset security • Multi-party analytics • Anonymous info sharing	• Genomics and Biopharma • Medical AI • X-Ray and scan image detection

The Problem: Online Growth Threatened by Digital Fraud

Shift to Online:

Today's consumers expect digital options from doctors, schools, jobs, and more. The same goes for banking.



It'll come as a surprise to no one that online and mobile transactions spiked in 2021.
LNRS, Jan 2022. *True Cost of Fraud.* U.S. Banks: Transaction Volume by Channel.

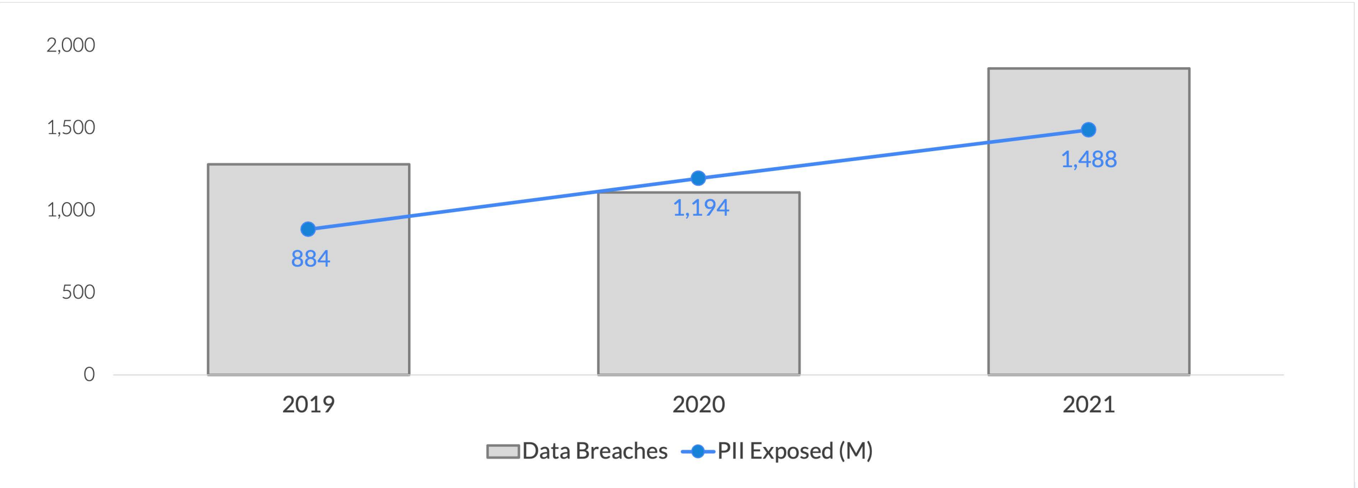
Rise in Fraud:

Along with this rise in online behavior – fueled in part by the Covid-19 pandemic – came a dramatic rise in digital fraud.

- Although digital transformation initiatives in financial services had been in motion for years, the pandemic forced banks to rush their development of online services.
- Along with a big target in the form of stimulus payments, this hasty growth of online services ushered in a boom in fraud.

Data Breaches & PII Exposed

Personally identifiable information (PII) is the fuel for digital fraud, and criminals have plenty to work with.

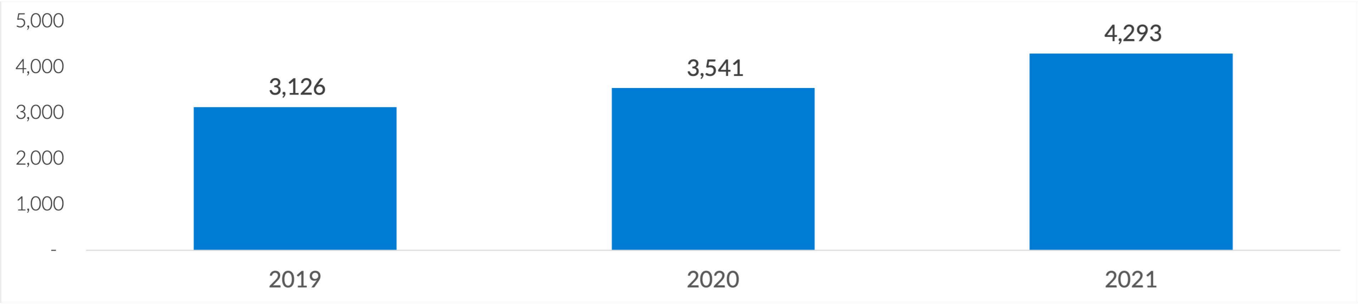


1.5 billion identity elements have been stolen over the past three years.

Identity Theft Resource Center, Jan 2022. *2021 in Review: Data Breach Annual Report.* https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

Suspicious Activity Reports

The steady rise in reports on a range of financial crimes makes it clear that new approaches are needed.

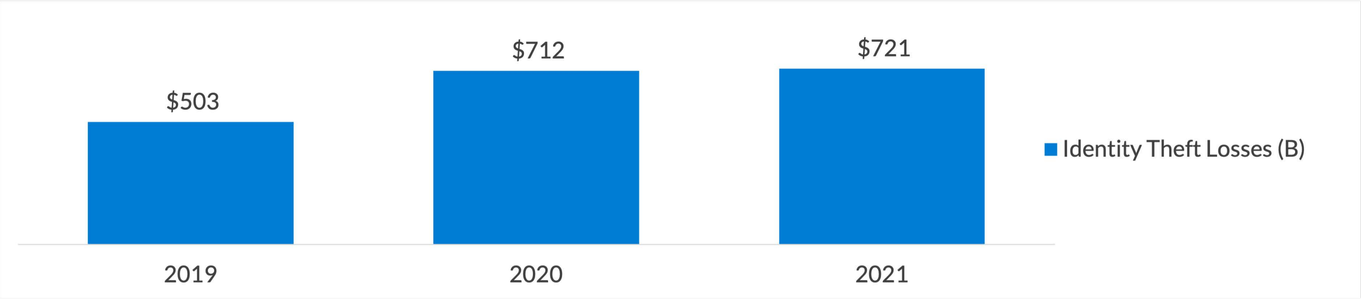


SARs increased by 21% over the record number of reports filed in 2020.

U.S. Treasury Financial Crimes Enforcement Network, 2014-2021. *Suspicious Activity Report Statistics.* Depository institutions only. https://www.fincen.gov/reports/sar-stats/

Identity Theft

The amount of losses from identity theft alone threatens the foundation of our payments system.

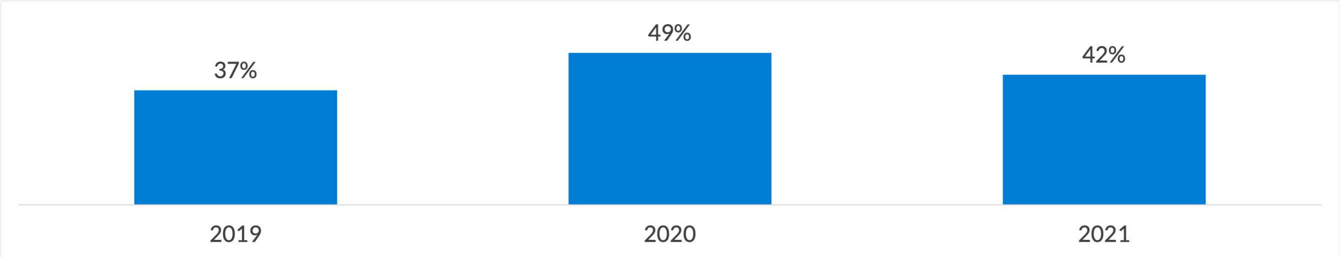


Following a sharp increase in 2020, identity theft losses also reached a new record in 2021.

Aite Group, Mar 2021. U.S. Identity Theft: The Stark Reality.
https://aite-novarica.com/report/us-identity-theft-stark-reality

Fraud's Success Rate

This swell in fraudulent activity is enabled by increasingly sophisticated approaches. In some cases, criminals use AI to bypass legacy fraud detection solutions, and leverage automation to operate at scale.



Over 40% of fraud attacks are successful.

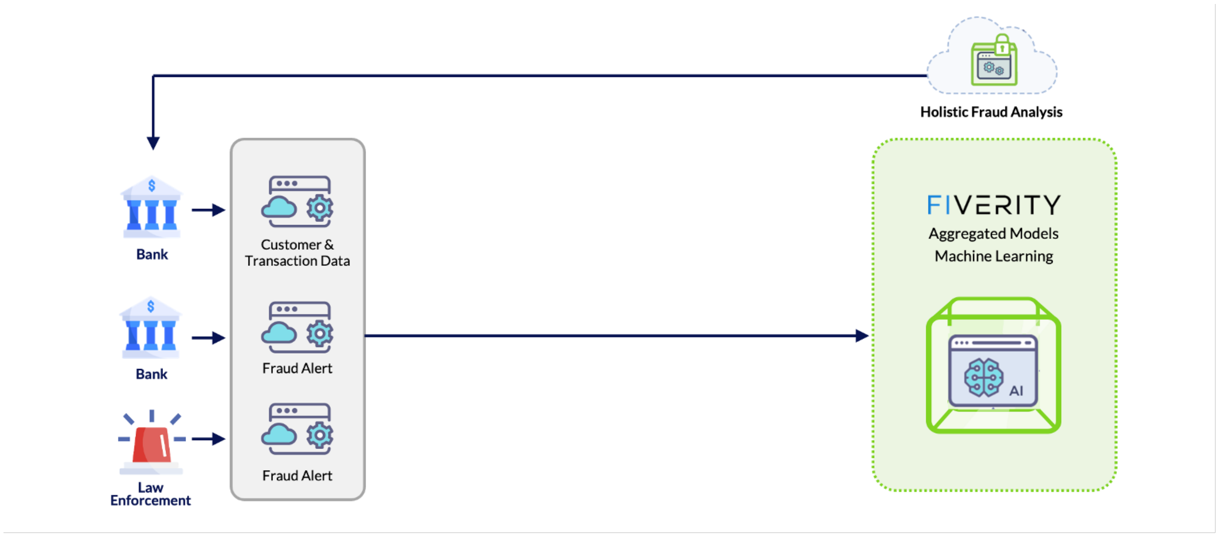
LNRS, Jan 2022. *True Cost of Fraud 2021.*

Neobank Growth Hits a Speed Bump

While neobanks have grown tremendously by offering online customers convenient, mobile-first technology, overwhelming volumes of fraud have put their entire business model in jeopardy.

Feb 2021	Payments processor blocks neobank transactions after finding 45% of ACH transfers are fraudulent
Mar 2021	Car rentals, hotels and other travel businesses decline transactions from neobanks
May 2021	Betterment blocks all new connections to accounts from neobanks
Jul 2021	Robinhood denies transfers from multiple neobanks as its provision for fraud losses increases 54%
Jun 2021	Chime locks undisclosed number of customers out of accounts
Sep 2021	Banks begin putting longer holds on cash transfers from neobanks
Jan 2022	Paypal closes 4.5 million illegitimate accounts
Feb 2022	Betterment freezes checking account applications due to fraud attempts

The (Partial) Solution: Holistic Fraud Analytics



Most financial institutions are forced to rely on a secure but limited data set to identify fraud, and lack real-time data on fraudulent activity.

Cloud-based fraud analytics provide:

- Access to a significantly larger data set
- Models that are constantly maintained by expert third parties
- Alerts to fraudulent activity identified by other banks or law enforcement

It sounds like a no-brainer, but security is of course the fly in the ointment...

Downside: Sensitive Data & Proliferating Threats

Data Privacy

The sensitivity of customer PII and transaction data is largely why banks are hesitant to participate in cloud-based models or share info with one another.

- Strict (and occasionally fuzzy) legal requirements: within the U.S. alone, rules regarding the protection of PII (including requirements for informing consumers when a data breach may have occurred) are maintained by different federal agencies and even different states. (Thanks, California.)
- Corporate responsibility and reputation: even if a company isn't legally responsible for a data breach, the risk of losing consumers' trust may be even more concerning.

Bad Actors

Although the image of the lone hacker is commonplace, there are a range of bad actors working independently and in groups.

- Hackers: use malware to exploit vulnerabilities in the hypervisor or operating system (OS)
- Malicious Insiders: anyone with escalated admin privileges and an axe to grind
- Third Parties: vendors and “frenemies” who stand to gain from confidential data

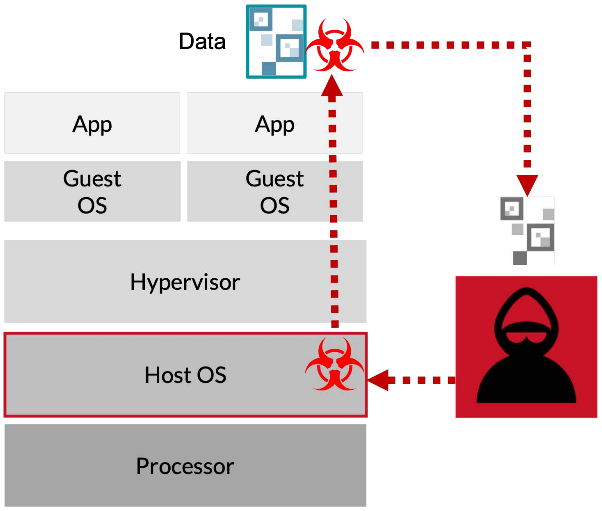
Insecure Environments

Full data protection requires unique protocols for each environment the data comes across.

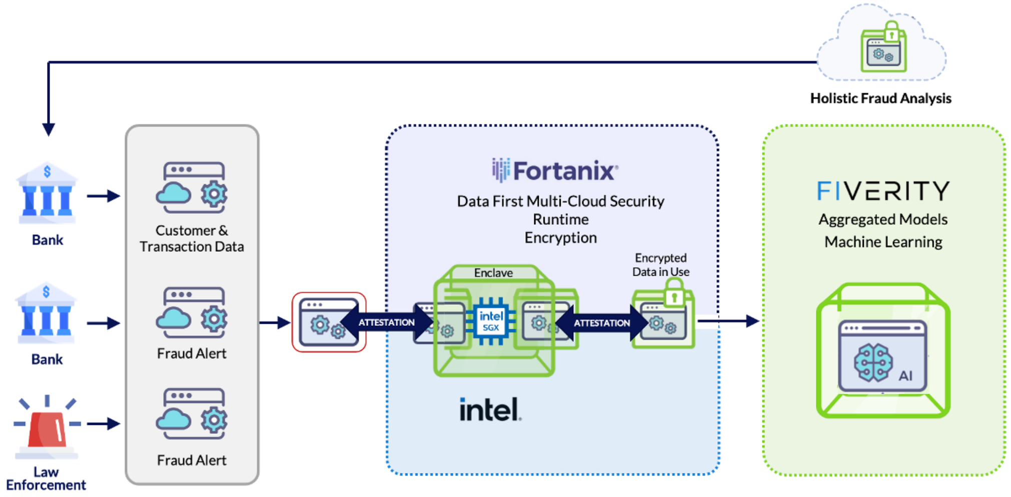
- At rest: ensuring encryption when data is stored
- In flight: ensuring encryption when data is transmitted
- In use: protecting data when it’s decrypted and exposed in system memory for active processing
  - This is the most challenging gap and is vital to maintaining full data security

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.



The (Complete) Solution: Holistic Fraud Analytics via Confidential Computing



By implementing Confidential Computing with Fortanix and Intel, FiVerity provides secure access to cloud-based analytics and allows banks to collaborate on fraud detection. The robust solution gives banks:

- Aggregated fraud detection algorithms
- Machine learning models that improve the algorithms over time
- Real-time alerts to fraudulent activity from other banks and law enforcement
- Full data security and control over information shared

What is Confidential Computing?

Confidential Computing represents a combination of software and hardware that gives financial institutions greater protection of sensitive customer data and improved control over its access. Put simply, Confidential Computing is the key to the secure models and collaboration financial institutions need to manage fraud while pursuing online growth.

Confidential Computing: How It Works

Confidential Computing has a critical role to play in enabling the secure sharing of sensitive data. While protocols exist to protect data in transit (moving over a network connection) and at rest (in storage and databases), Confidential Computing eliminates the remaining data security vulnerability by protecting data in use — during processing or runtime.

A Collaborative Effort

CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Computing isn't the brainchild of any one company – it's a joint initiative that includes a range of technology leaders, academics, government regulators and non-profits. This collaborative approach removes concerns of a single company fully owning and controlling this technology.

Trusted Execution Environments

Enclaves rely upon Intel® Software Guard Extensions (Intel® SGX), which applies hardware-enhanced protection to create Trusted Execution Environments (TEEs) to isolate and protect data during active processing. There are varying ways to develop TEEs, dependent on the size of the trust boundary and attack surface.

Enclaves

To enable runtime encryption, Confidential Computing runs applications in isolated environments called "enclaves." These enclaves are API driven and easily deployable – similar to any other cloud application.

Attestation

In addition to encrypting the data in use, enclaves also rigorously safeguard both the application and the data inside it using attestation. This is a process that verifies the security of an enclave, the application run inside it, and the data that is being processed.

For example, the Intel® Software Guard Extensions (Intel® SGX) attestation process helps an enclave to prove that:

1. The code built and validated by the user is running unmodified in a genuine enclave.
2. The hardware in which it is running is a secure platform with all the necessary updates.
3. The hardware and software configurations needed are correctly applied.

Why Confidential Computing is Set to Change the Game

Collaborative Modeling without Sharing Private Data

Confidential Computing provides secure access to aggregated fraud detection models.

- Financial institutions that had previously limited themselves to on-premise technology can confidently embrace cloud sharing and access collaborative learning models.
- These models analyze encrypted data from multiple banks to identify patterns of fraudulent activity with a much higher degree of accuracy. Information about fraudulent activity from each financial institution is provided anonymously.

Downsides: On-Premise Solutions

Due to concerns over data leaks, many organizations continue to limit their fraud detection efforts to on-premise solutions that provide a limited view of the fraud landscape:

- Relatively small data sets limit machine learning capabilities for improving models over time.
- On-premise detection models quickly suffer from degradation, becoming stale shortly after imple-mentation.
- Keeping up with changes in the data and accurately detecting emerging patterns requires ongoing attention on a larger scale.

Info-Sharing

Collective knowledge and expertise can be a company's best line of defense, especially when it comes to thwarting external threats. Until recently, a range of legal, competitive and technological concerns have limited the scope of information sharing across financial institutions. The adoption of Confidential Computing is set to change that.

This is crucial as regulators push for more information-sharing across banks to fight digital fraud. As the Federal Reserve stressed in a series of white papers on synthetic identity fraud:

> *"No single organization can stop wide-ranging, fast-growing synthetic identity fraud on its own. It is imperative that payments industry stakeholders work together to keep up with the evolving threat posed by synthetic identity fraud, which includes anticipating future fraud approaches."*

Info-Sharing Challenges Resolved

Here are three collaborative challenges that financial institutions previously faced, and how Confidential Computing can help.

1. Competitive Disadvantage

Fraud occurs at every bank, but that doesn't mean banks are eager to share their security lapses with competitors or regulators. If they did, however, they could pool their intelligence about fraudsters and help one another prevent further attacks.

Now that Confidential Computing offers the potential for secure but accessible data, banks can share critical, but appropriately limited, fraud intelligence. For example, when using FiVerity's Digital Fraud Network, Bank A does not have visibility to all of the fraudulent activity reported by Bank B. Institutions within the network are only alerted to identified fraudsters that attempt to become a customer or are already present in their portfolio.

2. Reputational Harm

Data leaks are always a legitimate concern, but Confidential Computing provides protection against internal leaks and external hacks. Internal access to the sensitive data is protected by hardware-level encryption enclaves, which protect information from malware and data breaches at the network, application and OS levels, and even from admins with physical access.

Data and code isolated in enclaves is even protected if the compute infrastructure is compromised. This is achieved via TEEs, which use hardware-backed techniques to increase security for code execution and data protection within that environment.

3. Privacy Requirement Violations

In addition to data encryption, Confidential Computing gives users a higher degree of control over the information shared – making inadvertent violations of privacy requirements less likely.

Embracing Confidential Computing

Financial institutions have been hesitant to adopt cloud technology for a number of reasons: the complexity of existing legacy solutions, skill gaps in the workforce, and fragmented compliance requirements. With digital fraud on the rise and regulators calling for a more collaborative approach, however, it is time for our industry to place secure, cloud-based models and intel-sharing at the heart of fraud management.

Digital fraud is a serious threat, but legitimate consumers and businesses are increasingly eager for the convenience that online banking solutions provide. With Confidential Computing, financial institutions have the secure tools needed to automatically detect fraud, so they can focus efforts on acquiring and assisting legitimate customers.

About Us

FiVerity: Holistic Fraud Analytics

Traditional banks entering the digital space, digital banks, and digital asset companies can feel confident with FiVerity. Our solutions are designed to support digital banking's growth with a comprehensive approach to fraud that verifies legitimate customers while detecting the latest fraudulent schemes.

FIVERITY

FiVerity's comprehensive approach strengthens fraud detection by integrating intelligence across anti-fraud and cybersec teams, existing vendors, and real-time marketplace activity.

FiVerity works with Fortanix and Intel to secure sensitive financial information via Confidential Computing. This solution gives banks secure access to powerful, cloud-based models that analyze data from multiple banks – identifying fraudulent patterns with a high degree of accuracy.

Fortanix: Data First Multi-Cloud Security

Fortanix® is a data-first multicloud security company solving the challenges of cloud security and privacy. Data is the most precious digital asset of businesses, but this data is spread across clouds, SaaS, applications, storage systems, and data centers. Security teams struggle to track, much less secure it. Fortanix empowers customers to secure all this data with a centralized solution. Its pioneering Confidential Computing technology means data remains protected at-rest, in-motion, and in-use, keeping it secure from even the most sophisticated attacks.

Intel: Confidential Computing Powered by Intel® SGX

Confidential Computing, powered by Intel® Software Guard Extensions (Intel® SGX), provides encrypted enclaves that break down data silos, not only within your organization, but with external entities—all without ever exposing the data to any of the parties.

For banks that have been hesitant to allow any sensitive data off-premises, Confidential Computing provides assurances that their data is fully protected. Unlike memory encryption technologies that leave data within the attack surface of the cloud stack, Intel® SGX provides a protected execution environment with a direct interface to the hardware. This limits access and minimizes the overall performance impact for both the application and other tenants on the server.

3rd Gen Intel Xeon Scalable processors drive Intel SGX technology

Featuring Intel SGX technology, 3rd Generation Intel Xeon Scalable processors provide advanced security capabilities that can be used in concert with existing infrastructure to enhance and protect the most sensitive portions of a workload or service. Intel SGX helps protect against many known and active threats by adding another layer of defense that reduces the attack surface of the system. Intel SGX's hardware-based memory encryption isolates specific application code and data in memory. Because sensitive information is partitioned into enclaves, it is secured from both external and internal threats, including higher-privileged processes. With Intel SGX, keys are protected as well, both at rest and in use, for added security whenever data is being processed. Only Intel SGX offers such a granular level of control and protection.