Transforming data security in Saudi Arabia with Intel® SGX

Intel® Software Guard Extensions (Intel® SGX) puts the software developer in the driver's seat with full control over which sensitive code and data needs an extra security layer when in use. The solution has been deployed for the first time in Saudi Arabia by one of a handful of certified cloud service providers, which needed maximum security for management of top-secret classes of client data.

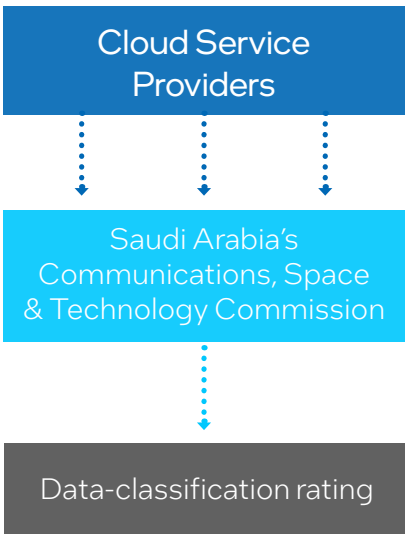
At a glance

- **Virtual Vision (V2)** deployed **Intel® Software Guard Extensions (Intel® SGX)** in March 2023. This cloud service provider has the highest certification level for secure management of data in Saudi Arabia, which enforces stringent data security and privacy laws.
- **Confidential Computing** powered by Intel® SGX addresses privacy and security concerns, even for the most sensitive classes of data. This is particularly important for tightly regulated management of government data in operating environments like Saudi Arabia's.
- **Intel® SGX** is a battle-hardened hardware-assisted security technology that significantly reduces the attack surface while giving the developer full control over an organization's unique security needs at the application layer.

Understanding Saudi Arabia's unique landscape

With businesses looking for trusted cloud service providers to help them balance effective digital transformation with data and privacy compliance, secure data management is critical. This is true not only for day-to-day handling of existing cloud-based data, but also for migrating data to a cloud environment.

One of the world's most stringent regulatory landscapes as far as data protection is concerned is Saudi Arabia. The Kingdom's **Cloud Computing Regulatory Framework** (CCRF) provides strict rules around management of client data for the country's cloud service providers (CSPs). Under the framework, CSPs must meet several specific requirements – one relating to how and where data is securely transferred, another about how security incidents are reported, for example.



CSPs must register with Saudi Arabia's Communications, Space & Technology Commission (CST, formally the CITC) and are given a data-classification rating that dictates the type of data they are legally allowed to deal with. Any breaches of the CCRF could result in the provider losing their operating license, with fines and further legal action also on the cards. Under the CCRF, Class (C) is the highest rating reserved for CSPs handling the most sensitive and private, top-secret government data. At present, **only 15 providers in the Kingdom have been cleared for Class (C) service provisions**, highlighting the high level of security that providers must deliver to land this privilege.

Unpacking challenges in strict regulatory environments

The cloud business model is one of shared responsibility between CSPs and application owners; the latter need security assurances from CSPs. This is particularly pressing considering **Saudi Arabia's Personal Data Protection Law** (PDPL). Businesses, like application owners, must be fully PDPL-compliant by September 2024 or face penalties. For example, unlawful use of sensitive data can lead to hefty fines and even the possibility of imprisonment.

Historically, software developers felt constrained by the security capabilities of major platform providers. Hackers are well versed in these same capabilities, exploiting weaknesses to steal sensitive data, credentials, or hijack code for attacks. With no means to apply a bespoke protection model to fit their own requirements, developers had to rely on the provider's security architecture.

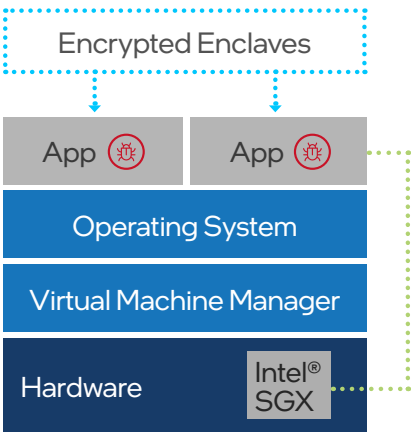
Intel® SGX addresses this issue. It is a new model that leverages the strengths of the platform and operating systems (OS) but delivers independence for the developer who understands what application secrets need additional protection to better meet regulations like the PDPL.

Meeting the need for an extra security layer

While typical security measures protect cloud-based data in storage and in transit, Confidential Computing technologies also **protect data while it's being processed.** However, when powered by Intel® SGX, Confidential Computing goes a step further by providing **encrypted 'enclaves'** that are designated by developers who have complete **control over which data and code needs special protection from disclosure or modification.**

Enclaves are created by isolating selected assets from the underlying infrastructure (hardware or OS) using hardware-level encryption. These secure containers are designed to protect against higher privilege-level processes including OS, virtual machines, and administrators. This innovative hardware-based trusted execution environment (TEE) delivers new Intel Architecture instructions that can be used by applications to help prevent direct attacks on executing code or data stored in memory.

The solution enables increased identity and records privacy, more secure browsing, stronger digital rights management (DRM), and hardened endpoint protection. It also allows developers to implement many high-assurance security use-cases that need to store secrets more safely or better protect data. An ideal proposition for CSPs serving clients who need to protect top-secret data within strict regulatory environments.



Over and above the **strengthened protection** for sensitive data that Intel® SGX enables, users are better able to stay **compliant** with stringent data-protection and privacy regulations. Furthermore, Intel® SGX delivers **cost and accessibility** benefits of cloud services without the security risks, while empowering developers to focus on **operation-enhancing innovation** and not security. Collaboration with other organizations to share, combine, and enrich sensitive data without ever exposing it is another benefit of the solution, which provides customers with unique operation-streamlining insights.

First real-world deployment in the Kingdom

Intel® SGX works on 3rd Generation Intel® Xeon® Scalable processors and further generations. Looking beyond the obvious benefits outlined above, it is also the most independently researched, hardware-based data center TEE in the market. There are **hundreds of active production deployments** of Intel® SGX across the globe, demonstrating real-world results that competitors are still unable to provide. This trusted technology was recently added to a portfolio of sophisticated solutions offered by Virtual Vision (V2), one of the select few Class (C) certified national cloud service providers in Saudia Arabia.

V2's offering entails seamless, secure access to business-critical cloud technologies, like **Intel® SGX, which they deployed in March 2023**. The transparent on-demand model that V2 delivers **empowers public- and private-sector organizations in the Kingdom** to adopt these technologies with reduced risk, helping them on their digital transformation journey. By leveraging Intel® SGX, V2's clients in Saudia Arabia can rest assured that their next-generation security environments will safely propel their business to new heights.

What features sets Intel® SGX apart?

There are eight that V2 customers are now able to enjoy. First, it offers **granular developer controls** for the creation of bespoke security set-ups, meaning hackers won't have the same level of insight that they would with standardized platform security, plus there's less exposed data for hackers to target with SGX significantly reducing area of attack. The **dedicated physical server** that Intel® SGX works on, with non-virtualized workloads, reduces the risk that comes with using a virtualized, multi-tenant cloud environment. The solution provides **unlimited data encryption keys per enclave, and the enclaves are large** (up to 1TB) on the new 3rd Gen Intel® Xeon® Scalable processors, allowing customers to handle larger code and datasets. Intel® SGX also enables users to take a faster and cheaper **'lift and shift' approach to cloud hosting**, and its familiar OS programming model means developers have lower learning curve as well.

Cloud-scale remote attestation and provision is yet another attractive feature of Intel® SGX. Ideal for helping ensure enhanced confidentiality and integrity, even in the presence of privileged malware at various layers like the OS, Basic Input/Output System, Virtual Machine Monitor, or System Management Mode. With this solution, the full cloud stack in the protected enclave remains outside of the trust boundary (as opposed to competitors' offerings where portions of cloud stacks must still be verified), which **significantly lowers the attack surface**. Finally, and increasingly important in our AI-driven world, is the fact that Intel® SGX is **interoperable with AI architectures** like federated learning where AI intellectual property shared for training is afforded greater protection. It can also be applied in various use-cases with emerging tech applications such as blockchain, and edge computing.

Products and Solutions:
Intel® SGX + 3rd Gen Intel® Xeon® Scalable processor

Industry: Cloud **Organization Size:** 51-200 **Country:** Saudi Arabia

Global solution that can be locally applied in any market

Intel® SGX is the next evolution of Confidential Computing, giving companies control over which data would benefit from an extra security layer. More than that, this hardware-based security technology helps protect data in use with the utmost care, making it a great fit even for public-sector organizations who manage top-secret data. At its core, Intel® SGX is helping businesses balance data-management compliance with digital transformation to strengthen productivity and reduce the security threat, leaving room for innovation.