Solution Brief

Thales and Intel® Collaborate to Enhance Trust in Confidential Computing

By Enabling End-to-End Data Protection

cpl.thalesgroup.com

THALES
Building a future we can all trust

Background information

Traditional data protection solutions were intended to secure data at rest and in transit on premises, or within trusted customer environments where access to the servers and the data was strictly enforced by the security policies of the organization.

With the emergence and adoption of shared storage and computing infrastructure or cloud services, and the subsequent disaggregation of capacity to the edge, new data security challenges are emerging, requiring additional security measures to protect the integrity of the data.

When customers use cloud services, the shared responsibility model governs the relationship between the cloud provider and their customers, where the cloud provider is responsible for the protection, access, and management of the infrastructure, and the customer is solely responsible for the protection of their own data and management of access to this data.

Therefore, new tools are required to protect customer data hosted in the public cloud. In addition to existing data protections for data at rest and data in transit, with Confidential Computing the data in use is also protected within an isolated environment, creating a comprehensive data protection for all the states of data at rest, in transit and in use.

Intel® and Thales are working together to enhance trust in public cloud deployments with Confidential Computing, by enabling customers to safely migrate their workloads to the public cloud and providing additional security controls that supplement the controls offered by the cloud provider.

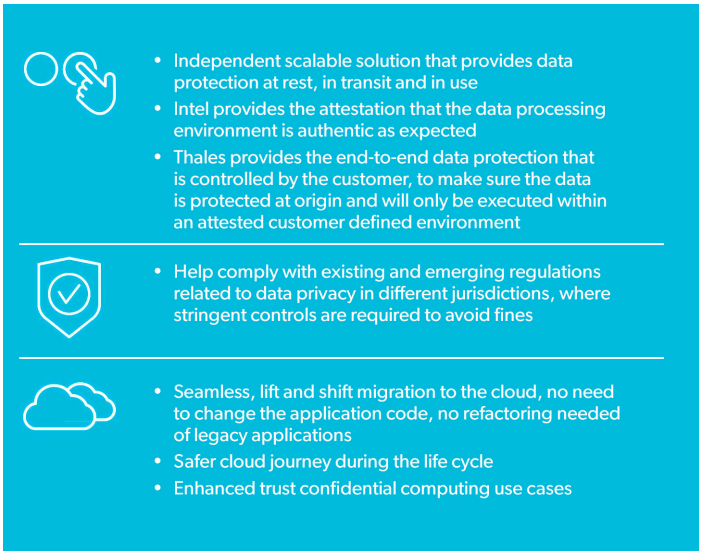
Thales and Intel®'s vision is to make Confidential Computing commonplace, adding protection capabilities for data in use with Intel®'s Confidential Computing and cloud-independent attestation services to Thales' CipherTrust Data Security Platform. Intel® announced this collaboration during their main annual event Intel® Innovation 2023, on September 19-20, in San Jose, California.

What is this collaboration about?

This collaboration enables:

- independent verification of the environment where the data will be computed
- the protection of data in use, also known as confidential computing
- complete customer end-to-end control of their data through its entire usage cycle

The organic data protection expansion of Thales CipherTrust Data Security Platform to provide End-to-End Data Protection capabilities over a Confidential Computing environment complements the platform's current market-leading data protection solutions for data at rest and in motion.



Intel® Tiber™ Trust Authority is a cloud-provider-independent SaaS attestation service for Confidential Computing used to verify the authenticity of the hardware and software stack of the Trusted Execution Environments (TEE) where the customer data will be safely processed in the cloud.

What is the problem this new solution solves?

Enterprises face multiple challenges to safeguard the privacy and integrity of their sensitive workloads. In addition to security threats, they need to comply with existing and emerging data security, privacy, and resilience regulations (e.g., DORA, NIS2, GDPR, PCI, UK-PRA Prudential Regulation Authority, among others), internal security compliance policies, and manage hybrid deployment environments on premises and in multiple clouds.

One of those challenges is migrating sensitive workloads to the cloud securely. Confidential Computing protects data while in use. Computations on the data are performed in an isolated hardware-based Trusted Execution Environment (TEE), removing, or reducing the ability for non-authorized parties to access code and data while being executed. Current cloud native Confidential Computing deployments lack of separation of duties, where external additional data security and verification controls required by enhanced trust Confidential Computing.

The separation of duties is an important security principle when the responsibility is shared between different parties. While most cloud providers offer native data protection features, the Shared Responsibility Model dictates that the ultimate onus of safeguarding sensitive data rests with the enterprises/organizations. Therefore, separation of duties is considered a best practice to help avoid security or privacy incidents and errors. For example, when managing keys in the cloud, many customers require a separation of duties between their encryption key management and the management of

sensitive data stored in the cloud to comply with data sovereignty requirements. In response, Thales and its cloud provider partners have co-innovated to develop Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) services. Similarly, the certification (attestation) of Confidential Computing secure enclaves should not be done by the cloud provider within the cloud provider environment. The joint solution from Thales and Intel® enables enterprises/customers to remain in control of their data protection, ensuring that sensitive workloads are never decrypted outside of a genuine certified Confidential Computing secure enclave enabling End-to-End Data Protection.

This collaboration between Thales and Intel® enables advanced customer controls around Confidential Computing use cases, such as End-to-End Data Protection—for data protection at rest, in motion, and in use—to secure customers' sensitive workloads on premises, during migration to the cloud, and in the cloud for storage and processing, while allowing the enterprise to stay in control of their data thereby separating this role from the cloud provider. Separation of duties (control) is especially important for highly regulated industries, the public sector, national security, and other verticals where data protection is paramount to safeguard the privacy of the information.

How does end-to-end data protection work?

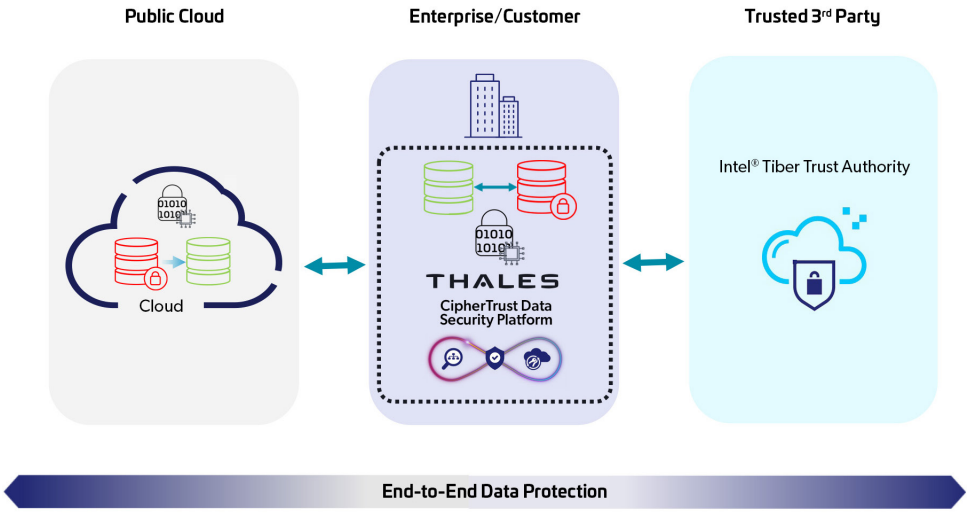
- When an enterprise customer needs to migrate workloads to the cloud that are sensitive in nature, such as personal identifiable information, trade secrets, financial data, intellectual property, datasets, AI models, or any valuable information sensitive workload, to reduce breaches outside the customer trusted data center, the customer needs to protect this data by advanced encryption to safeguard its privacy and integrity before the data leaves its trusted data center or network. Therefore, the customer's sensitive workload is initially encrypted at the enterprise end, within the data center, using the Thales CipherTrust Data Security Platform. Now the protected workload is ready to be shared and migrated to the cloud.
- When the enterprise/customer requires execution of its data at the Cloud end, this workload is moved into a Confidential Computing Trusted Execution Environment (TEE). Prior to starting the confidential VM inside the TEE, Thales CipherTrust Manager requests the attestation of this TEE to Intel® Tiber™ Trust Authority. After the attestation is performed, and the integrity of the TEE is confirmed as per defined customer policies, CipherTrust Manager applies customer defined data protection policies to enable the execution of the customer workload inside Confidential Computing Trusted Execution environment to start processing.

Potential use cases

- End-to-end Cloud Migration of Legacy Workloads. Safe lift-and-shift to the cloud, without refactoring, of legacy workloads can seamlessly enable use cases such as confidential multi-party collaboration, infrastructure security, confidential AI.
- Confidential Multi Party Collaboration. For example, in healthcare to facilitate the diagnosis of diseases and the development of pharmaceutical drugs, hospitals and healthcare facilities can contribute patient datasets to train a machine learning model. Each facility that contributes to training the model can use it and receive useful results without seeing the other party's sensitive data.
- Confidential AI. For example, in banking to detect money laundering, multiple banks can share data (customer datasets) without exposing their customers' personal data. Banks run analytics on the combined sensitive datasets that can detect the movement of money by one user between multiple banks without the banks accessing each other's data.

Partners

End-to-End Data Protection provided by Thales and Intel® means that enhanced trust in Confidential Computing and associated services are available with Intel® Trust Domain Extensions (TDX) confidential VMs hosted by both Google Cloud and Microsoft Azure.



End to End Data Protection to enhance trust in confidential computing

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us