Solution Brief

THALES

CYBERSECURITY

intel

Microsoft

Thales, Intel, and Microsoft Collaborate to Enhance Trust in Confidential Computing

By Enabling End-to-End Data Protection

cpl.thalesgroup.com

THALES

CYBERSECURITY

intel

Microsoft

Thales, Intel, and Microsoft are collaborating to deliver an end-to-end confidential computing solution that empowers enterprises to protect sensitive data across all environments. By uniting industry-leading security, independent verification, and robust data protection for information at rest, in transit, and in use, this partnership helps organizations confidently manage confidential AI, meet regulatory requirements and mitigate risks as they move critical workloads to the cloud.

Leveraging Azure, customers can advance confidential AI initiatives by safeguarding their models and intellectual property and enabling secure collaboration between organizations, ensuring sensitive information remains protected throughout the process.

The Challenge

Enterprises must protect sensitive workloads and comply with evolving regulations like GDPR, DORA, NIS2, and PCI-DSS. As data moves across on-premises, hybrid, and multi-cloud environments, privacy and compliance challenges increase. Migrating critical workloads to the cloud introduces new risks, as traditional protections for data at rest and in transit are often insufficient in public and shared infrastructures.

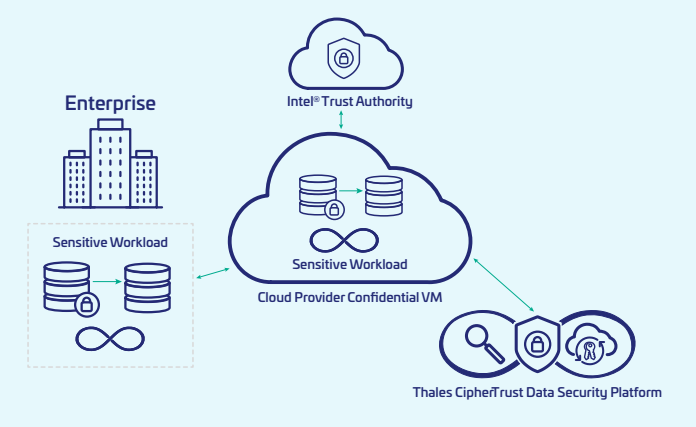
Confidential Computing protects data in use within secure, hardware-based enclaves, reducing unauthorized access during processing. However, most cloud-native solutions lack strong separation of duties and independent verification—essential for greater trust. Under the shared responsibility model, providers secure infrastructure, but enterprises remain fully responsible for data protection.

Thales, Intel, and Microsoft collaborate to fill these gaps, enabling secure migration of sensitive workloads to the cloud with comprehensive controls for all data states. Their joint solution delivers advanced, scalable confidential computing designed to meet enterprise security and compliance needs.

The Joint Solution

Traditional data protection strategies were developed to secure data at rest and in transit within on-premises or trusted customer environments, where access to servers and information was governed by stringent organizational security policies. The introduction of shared storage, cloud services, distributed computing infrastructure, and resource deployment at the edge has brought about new challenges that necessitate advanced security measures to ensure data integrity.

Within cloud service models, the shared responsibility framework delineates provider and customer roles: providers manage infrastructure protection, access, and management, whereas customers assume responsibility for safeguarding their data and administering access controls. This evolving landscape demands innovative solutions to protect customer information residing in public cloud platforms. Confidential Computing builds upon traditional data protections by securing data in use within isolated environments, thus ensuring comprehensive coverage across all data states.



End-to-end Data Protection to enhance trust in confidential computing

The partnership between Thales, Intel, and Microsoft delivers:

- independent verification of the data computing environment
- robust protection of data in use via confidential computing techniques
- complete customer oversight of data throughout its lifecycle

Comprehensive Data Protection with Thales CipherTrust in Confidential Computing

The Thales CipherTrust Data Security Platform now offers expanded capabilities for end-to-end data protection in confidential computing settings, complementing its existing provisions for data at rest and in transit. Intel® Trust Authority is a SaaS attestation tool independent of cloud service providers, enabling the verification of hardware and software stacks within trusted execution environments (TEEs) that process sensitive customer data in the cloud.

Separation of duties stands as a fundamental principle when responsibilities are distributed among multiple stakeholders. While Microsoft and other cloud providers include integrated data protection solutions, the Shared Responsibility Model ultimately assigns enterprises the obligation to safeguard sensitive information.

Adopting separation of duties as a best practice helps mitigate security and privacy risks.

Certification of confidential computing secure enclaves should not be exclusively conducted by the cloud provider within its infrastructure. The joint solution from Thales and Intel empowers enterprises to manage their own data protection mechanisms, ensuring that sensitive workloads remain encrypted except when processed inside certified secure enclaves

The collaboration among Thales, Intel, and Microsoft grants customers greater control over confidential computing scenarios, encompassing data protection for data at rest, in transit, and in use. This enables organizations to maintain security of sensitive workloads whether locally, during migration, or in the cloud for storage and processing, while retaining authority over their data independent of the cloud provider. Separation of duties proves essential for regulated sectors, government entities, national security, and other areas with critical data privacy requirements.

End-to-End Data Protection Explained

When an enterprise needs to migrate sensitive workloads to the cloud that contain AI models, personal data, financial information, or trade secrets, it must encrypt this data to reduce breaches. Using Thales CipherTrust Data Security Platform ensures privacy and integrity before the data leaves its trusted network. The encrypted workload is then ready for secure cloud migration.

When an enterprise needs to run data in a Cloud TEE, the workload is moved to a Confidential Computing TEE. Before the confidential VM starts, Thales CipherTrust Manager requests Intel Trust Authority to attest the TEE's integrity and security. If the TEE passes attestation per customer policies, CipherTrust Manager enforces the data protection policies, allowing secure workload execution in the TEE.

Real-World Applications of Confidential Computing

- Confidential AI, for example in banking, multiple banks can share data (customer datasets) without exposing their customers' personal data to detect money laundering. 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.
- End-to-end cloud migration, with safe lift and shift, without refactoring, of legacy workloads to seamlessly enable use cases such as, among others, confidential multi-party collaboration, infrastructure security, confidential AI.
- Multi-party collaboration with confidential computing, such as 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.

End-to-end data protection for these scenarios ensures a higher level of trust in confidential computing, leveraging Intel® TDX confidential virtual machines hosted on Microsoft Azure - available today for production deployments across both general-purpose (DCesv6, DCedsv6) and memory-optimized (ECesv6, ECedsv6) VM series - and related services. These VMs comprise Intel® AMX for AI acceleration.

Take the Next Step Toward Advanced Data Protection

Discover how confidential computing can transform your organization's data protection strategy. Visit our Microsoft marketplace listing for more details or contact Thales for a personalized demonstration or consultation.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Member of
Microsoft Intelligent Security Association
Microsoft Security

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us