Solution Brief
Intel Security

Microsoft Deploys Confidential Computing To Protect $25B per Year in Customer Payments

Software giant moves credit card transactions to Azure Cloud Services running Intel® Software Guard Extensions (Intel® SGX)

Walking their talk

Microsoft is a Fortune 15 company and among the world's foremost software and cloud service providers. With their vast global customer base, the company processes millions of credit card payments for their products and services, totaling over $25 billion annually. To say that the security of their transaction system is critical to their business is an understatement.

To ensure the success of the vital function of processing payments, Microsoft's Commerce Financial Services was empowered to design, build, and implement a payment gateway solution that delivers the highest degree of reliability, security, and compliance. For years, the company used application-specific, on-prem infrastructure for payment processing, but in 2023 the team began implementation to switch to a cloud-based solution using Azure Confidential Computing enabled by Intel SGX. After careful consideration, Microsoft determined that Azure Confidential Computing met all of their requirements for scalability, uptime, and cost-effectiveness, while also exceeding security and regulatory standards.

Microsoft's commitment to the new cloud-based payment solution offers the strongest possible testimony to their confidence in the scalability and security of Azure Confidential Computing and Intel SGX. By deploying a Payment Card Industry Data Security Standard (PCI-DSS) Level 1-compliant processing and vaulting solution on Azure, Microsoft's Commerce Financial Systems (CFS) passed a critical milestone in their drive to post 100% of their payment services on Azure. Microsoft has made a powerful statement that Confidential Computing technology is mature and ready to scale.

The solution breaks new ground in the secure processing of payments in the public cloud. It enables stronger confidentiality and security in the payment solution space by increasing assurance that both payment instruments and the private key material used to protect them are always encrypted and protected—not only at rest and in transit, but while actively in use during processing as well.

	Traditional Encryption	Traditional Encryption + Confidential Computing
Data at rest: Encrypt inactive data in the payment system when stored in blob storage, database, etc.	✓	✓
Data in transit: Encrypt payment system data flowing between untrusted public or private networks	✓	✓
Data in use: Protect/encrypt payment system data in use, while in RAM, and during computation		✓

Built on top of existing Azure enterprise technologies such as Azure Firewall Premium, Azure Kubernetes (AKS), Azure Key Vault Managed HSM, and Microsoft Entra ID, the new solution meets or exceeds current PCI-DSS standards for data protection and access control. This is made possible by Intel SGX technology, which uses hardware-enhanced capabilities built into Intel® Xeon® processors, designed to limit access to sensitive data actively in use in the CPU and memory. Only code that has been attested as genuine and unaltered is allowed to access confidential data. With Intel SGX enclaves, Microsoft helps protect the crucial encryption key operations that its payment system depends on for high security and confidentiality.

Microsoft recognized several primary requirements for the payment system. First, they wanted to limit the size of their Trusted Computing Base (TCB)—the code allowed to access sensitive payment data—to the smallest possible size. Second, they wanted to deploy confidential code modules in standard containers, not separate VMs.

Intel SGX strives to meet both these critical requirements, while also addressing other key issues. For instance, in their previous system, Microsoft processed payments through an on-prem solution that used purpose-built hardware. That meant they could not responsibly port the system to the cloud because it simply couldn't provide the end-to-end protection required. The availability of Intel SGX on Azure changed that. The new system leverages the scalability and agility of the cloud while increasing overall security by protecting data in memory. Microsoft generated $2 million in Hardware Security savings by moving from on-prem infrastructure to the cloud. In addition, the solution significantly decreased OpEx by helping reduce costly cryptographic asset transfers around the world.[1]

Confidential Computing includes application process level isolation through Intel SGX, using processor-level memory encryption available on Azure DCsv3 and DCdsv3 instances. This confidentiality solution delivers protection of data *in use* by processing that data in a hardware-based, attested Trusted Execution Environment (TEE)—adding to existing platform capabilities of encryption *in transit* and *at rest*.

These products help enable even the most security-sensitive workloads to be safely deployed in public Azure without the need for sovereign, dedicated, or hybrid on-prem solutions.

Figure 1 illustrates how Azure Confidential Computing encrypts data in memory in the hardware-based TEEs that protect data in use. The interaction of an Intel SGX application enclave node pool running on AKS with a managed HSM helps ensure the highest degree of data security and privacy for the sensitive information customers trust Microsoft to safeguard—and everything is handled in the public Azure cloud.

Intel: The leader in hardware-based cloud security

Cloud security encompasses technologies in both the hardware and software layers that enable Confidential Computing online. Intel zero-trust security solutions accelerate cryptography, help ensure applications run as expected, establish a root of trust in the firmware layer, and deliver tamper-resistant storage. This commitment to security can enable businesses to discover and profit from the transformative value of the cloud.

Microsoft's commitment to running their business-critical credit card processing system on Azure with Intel SGX underscores the value Intel technology delivers.

As leaders in Confidential Computing, we can help you scale even your most critical business workloads to the cloud. Contact your Intel representative for more information.

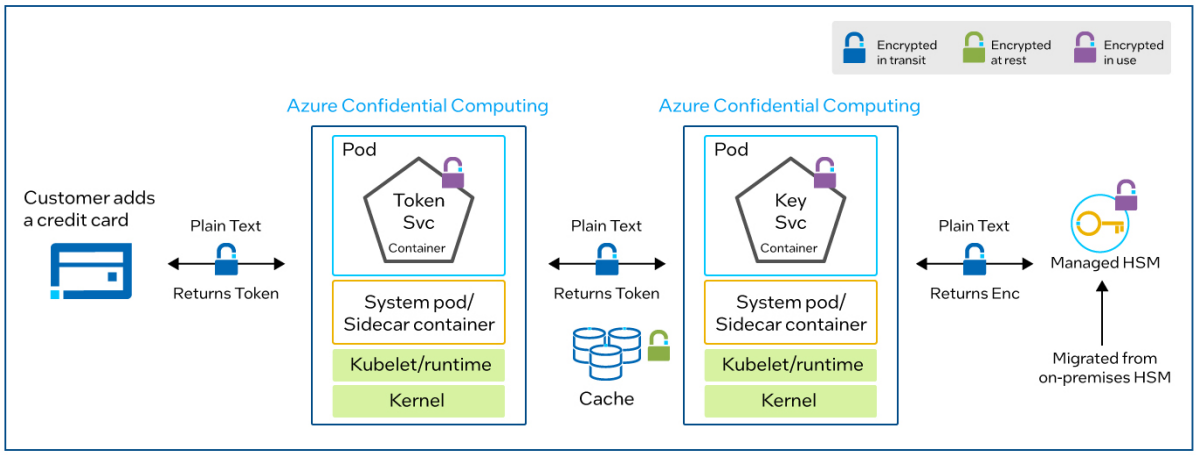

Figure 1. Payment Infrastructure using Azure Confidential Computing

Learn More

Intel Confidential Computing products include:	
Intel® Software Guard Extensions (Intel® SGX)	**Application Isolation** The most deployed, researched, and updated Confidential Computing technology on the market today. Trusted Execution Environments (TEEs) based on Intel SGX help protect data while it is actively processed in memory.
Intel® Trust Domain Extensions (Intel® TDX)	**VM Isolation and Protection** New functionality available through select cloud providers offers increased confidentiality at the virtual machine (VM) level, enhancing privacy and control over data.
Intel® Trust Authority	**Zero Trust Attestation** Take Confidential Computing to the next level with a Zero Trust attestation SaaS that verifies the trustworthiness of compute assets at the network, edge, and in the cloud.

Intel Confidential Computing
https://www.intel.com/content/www/us/en/security/confidential-computing.html

Intel® Software Guard Extensions
https://www.intel.com/content/www/us/en/products/docs/accelerator-engines/software-guard-extensions.html

Intel® Trust Domain Extensions
https://www.intel.com/content/www/us/en/products/docs/accelerator-engines/trust-domain-extensions.html

Intel® Trust Authority
https://www.intel.com/content/www/us/en/security/trust-authority.html

Azure: Intel SGX Enclaves
https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-computing-enclaves

Microsoft Blog: Announcing the Move to Azure
https://techcommunity.microsoft.com/t5/azure-confidential-computing/announcing-microsoft-moves-25-billion-in-credit-card/ba-p/3981180

Azure Confidential Computing
https://azure.microsoft.com/en-us/solutions/confidential-compute

Azure Managed HSM Overview
https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

Confidential Computing Application Enclaves on Azure Kubernetes
https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-nodes-aks-overview

Solution Brief Provided by Intel

ACG6945MAI