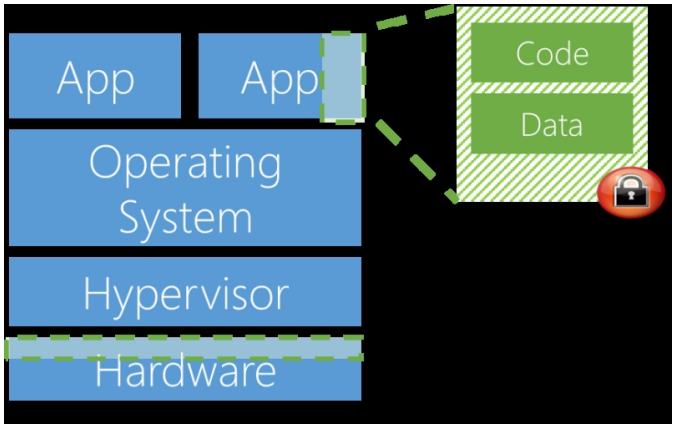
Microsoft proposes a a boost in security for the Azure cloud platform-- Confidential Compute, a feature allowing applications running on Azure to keep data encrypted even when being computed in-memory.



Azure already encrypts data while at rest at in transit, but the encryption of data while in an in-use state eliminates a potential weak link in the security process. After all, data loses all protection when it is is processed by applications, meaning hackers can potentially access it via malware.

"Confidential Computing ensures that when data is "in the clear," which is required for efficient processing, the data is protected inside a Trusted Execution Environment (TEE)," a Microsoft blog post reads. "TEEs ensure there is no way to view data or the operations inside from the outside, even with a debugger. They even ensure that only authorised code is permitted to access data."

Microsoft offers two TEE technologies-- a software-based Virtual Secure Mode in Hyper-V components in Windows Server 2016 and Windows 10, and Intel Software Guard Extensions (SGX) technology built in the processors running on Azure cloud servers. The future should see other types of TEEs through additional software and hardware partners.

Microsoft is also supplementing the Always Encrypted feature in Azure SQL Database and SQL Server with Coco Framework, the open-source confidentiality system used in enterprise blockchain networks.

Azure Confidential Computing is currently available through an early access program.

Go Introducing Azure Confidential Computing