

VM-Level Trusted Execution Environment

Sensitive
Data

Customer
Application



Operating System

Encrypted Memory
(Confidentiality and
Integrity)

Hardware Interfaces

Virtual Machine
Manager

Trusted CPU
Features



Untrusted Cloud Platform