Secure Encrypted Virtualization (SEV)

Return to Glossary

Secure Encrypted Virtualization (SEV) integrates main memory encryption capabilities with the existing AMD-V virtualization architecture to support encrypted virtual machines. Encrypting virtual machines can help protect them not only from physical threats but also from other virtual machines or even the Hypervisor itself. SEV thus represents a new virtualization security paradigm that is particularly applicable to cloud computing where virtual machines need not fully trust the hypervisor and administrator of their host system. As with Secure Memory Encryption (SME), no application software modifications are required to support SEV.

Source:
https://developer.amd.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf