AMD DATACENTER SOLUTIONS

Solving the Cloud Trust Problem with WinMagic and AMD EPYC™ Hardware Memory Encryption

White Paper
October, 2018

Introduction

Enterprises today are reluctant to move their most sensitive data into the cloud because of concerns with:

- Confidentiality of data-at-rest and data-in-use
- Exposure to other tenants
- Cloud service provider admin access
- Cloud infrastructure vulnerabilities
- Undisclosed government access

The cloud service provider is similarly concerned because they have the liability of potential access to customer data. They need to spend time and money on expensive controls to obtain certifications to build trust, but still have potential exposure to customer data.

The solution to both the trust and liability problem is for the cloud service provider (CSP) to not have access to customer data, not even CSP administrators or hypervisors. Encrypting both the storage and memory of a virtual machine is the answer, so long as the customer controls the process – not the CSP.

Cloud Data Encryption

Virtual machines running in the cloud need virtual volumes or disks for storing data. This offers a security challenge as this data may be susceptible to unauthorized access by cloud provider insiders or be moved to other jurisdictions or be subject to requests for access by governments. Thus, it would be a good idea to encrypt this data. The key questions are "**Who encrypts the data?**" and "**Who manages the encryption keys?**"

Three different methodologies are summarized in Table 1.

Method	Encryption performed by	Keys owned and managed by
SSE *Server-Side Encryption*	**cloud provider**	**cloud provider**
SSE-CPK *Server-Side Encryption with Customer Provided Keys*	**cloud provider**	**customer**
Client-Side Encryption	**customer**	**customer**

Table 1. Methods of cloud volume data encryption.

SSE

"Server-Side Encryption" protects the data when the cloud service provider recycles the underlying physical storage. It doesn't protect against insider attack. It also is susceptible to governments which may require the cloud service provider to use their copy of the encryption keys to decrypt the data without the customer's knowledge.

SSE-CPK

"Server-Side Encryption with Customer Provided Keys" provides more protection than SSE. While the cloud provider still performs the encryption, the customer provides and manages the keys. The cloud service provider promises to only keep the keys in its hypervisor memory while the virtual machine is up and running. However, the keys still flow through cloud provider interfaces and it is not difficult to divert these to disk.

Client-Side Encryption

Client-side encryption occurs in the cloud, but it is performed by the customer's virtual machine not the cloud's hypervisor. Sometimes this is called "in-guest encryption". The customer selects the encryption method and provides the encryption software. Most importantly the customer owns and manages the encryption keys. The customer could hide the keys in an unencrypted portion of the volume, but the better approach is for the customer to store and manage the keys on their own premises.

The Need for Cloud Memory Encryption

Despite the advantages of client-side encryption, there is still a concerning security problem. While running, the virtual machine will have the encryption keys in memory. This memory could be attacked, and a determined adversary could even retrieve the data encryption key used to encrypt the drive. In fact, there is a lot more information in memory than just keys. At one point or another, most of the data on the drive will have been processed in memory. Gartner recently discussed this in *Key Management as a Service Exposes Different Risks to Data in Public Clouds*[1]. This "data in use" could be vulnerable to unauthorized access, insider threats or hypervisors hacks and vulnerabilities.

[1] https://www.gartner.com/doc/3839363/key-management-service-exposes-different

WinMagic + AMD

To address this data-in-use security concern, AMD introduced hardware memory encryption capabilities in its EPYC processors. The Secure Encrypted Virtualization (SEV) feature uses multiple keys to cryptographically isolate virtual machines and the hypervisor from one another.

An attacker with hypervisor administrator access or a compromised VM account may try to read the memory of other virtual machines. With SEV, the attacker sees only encrypted data. WinMagic is building upon the foundation of encrypted memory with WinMagic SecureDoc™ CloudVM[2] .

When a virtual machine boots up in the cloud it loads WinMagic's proprietary pre-boot environment. It first verifies and authenticates the cloud VM environment, enforcing policy that CloudVM must only run on hardware with encrypted memory. It then opens a secure connection to the customer's on-premises key manager. The key is transferred through the network and stored in encrypted virtual machine memory.

The key is used with SecureDoc CloudVM FDE (Full Drive Encryption) to access the encrypted disk volume, protecting data at rest, while memory encryption protects data-in-use including the disk encryption keys.

When addressing the issue of cloud data security, AMD's hardware memory encryption and WinMagic's SecureDoc CloudVM work together to provide a powerful combination of client-side encryption, on-premises key management, and hardware memory encryption.

To view a 3-minute demonstration of WinMagic's CloudVM for Linux proof of concept running with encrypted memory on an AMD EPYC processor, visit the link here: https://www.youtube.com/watch?v=I-tcJc4En5k

Authored by: Garry McCracken (CISSP), WinMagic
Brent Hollingsworth, Advance Micro Devices, Inc.
October, 2018

[2] https://www.winmagic.com/products/enterprise-server-encryption

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions and typographical errors. AMD reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of AMD to notify any person of such revisions or changes.

DISCLAIMER: THE FOREGOING GUIDANCE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OF INTELLECTUAL PROPERTY, OR FITNESS FOR ANY PARTICULAR PURPOSE. AMD CONTINUES TO INVESTIGATE THESE AND OTHER MITIGATION TECHNIQUES AND MAY MODIFY OR UPDATE THE INFORMATION IN THIS DOCUMENT WITHOUT NOTICE.