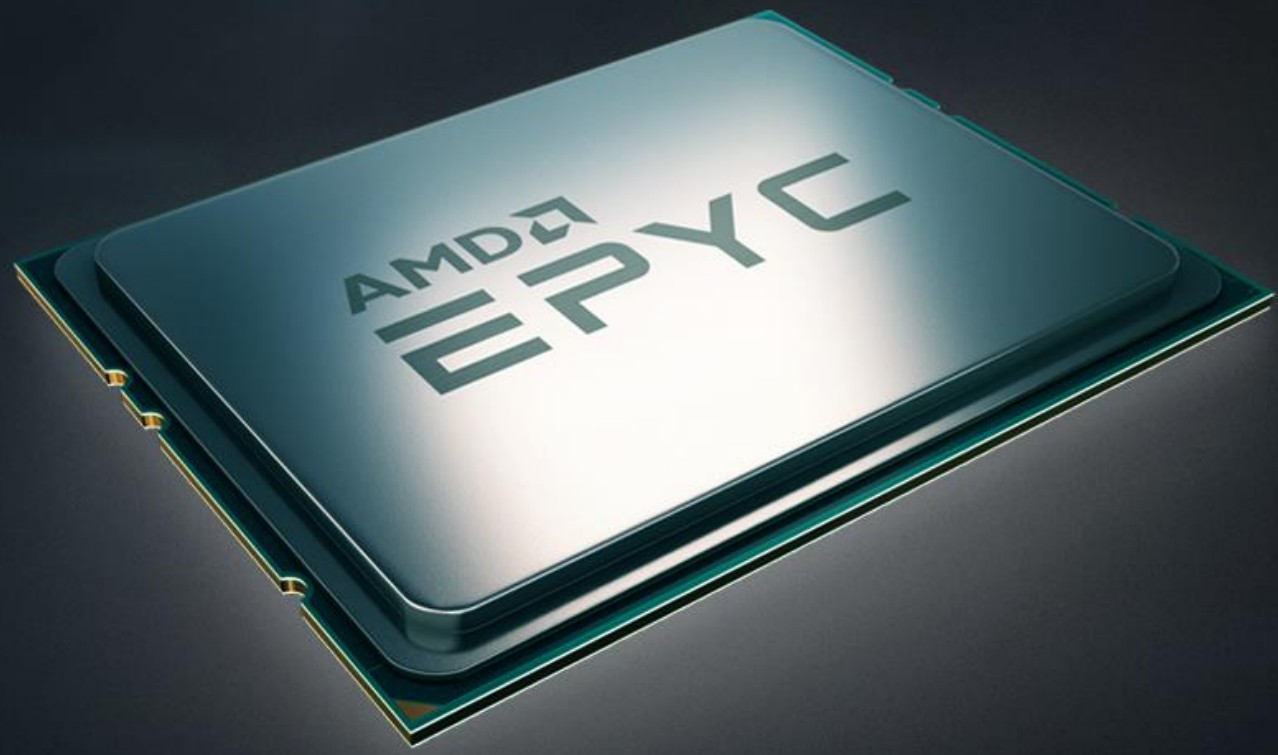
SECURE THE CLOUD WITH THE NEW AMD EPYC PROCESSOR

ANDRE HEIDEKRUEGER

March 2018

WHY SECURITY AT THE PROCESSOR?

- Software based security solutions can provide a layer of protection, but may ***still leave servers vulnerable*** – especially to internal attacks
- New X86 instruction set based solutions are limited in scope and ***require changes to applications***
- AMD has taken a ***unique Hardware based solution*** approach, which can protect against internal and external threats and ***does not require any changes to applications***



AMD EPYC™ - SECURITY STARTING AT THE PROCESSOR

HOW VULNERABLE ARE YOUR SERVERS?

- Servers can be vulnerable to physical attacks
  - Reset/Reboot attacks; Removal of DIMMS/NVDIMMs; I/O & Direct Memory Access (DMA) Attacks
- Attackers can extract sensitive information
  - Bank account numbers; Personal data; Credit card numbers; Secret keys…
- Anyone can execute
  - These attacks do not require high skill levels or sophisticated attack tools and can be executed by anyone with physical access to hardware

AMD SECURE MEMORY ENCRYPTION (SME) HELPS PROTECT YOUR DATA FROM PHYSICAL ATTACKS

IS YOUR DATA SECURE?

- $7M – The average total organizational cost of a US data breach in 20161
- It’s not just external threats
  - Attacks can come from Rogue Administrators or VM Breakout exploits
  - Over 40% of malicious attacks come from internal sources2

AMD SEV HELPS PROTECTS YOUR DATA AGAINST INTERNAL AND EXTERNAL THREATS

WHAT SHOULD YOU DO?

- Software and X86 instruction set based security solutions provide a layer of protection, but may not address all threats effectively and require changes to applications

- Implementing AMD's unique hardware based solutions, SME and SEV, can help protect against:
  - Physical attacks
  - Internal and external threats
  - Do not require changes to applications

TEST AMD SECURITY SOLUTIONS IN YOUR ENVIRONMENT TODAY

Details

AMD EPYC SECURE MEMORY ENCRYPTION (SME)

DATA PROTECTION WITH NO CHANGES TO SOFTWARE - PERFECT FOR ***EDGE COMPUTING DEPLOYMENTS***

Why do you need SME?	***Protects against physical attacks*** such as: • ***Reset/Reboot attacks***: Attacker inserts a USB key and then reboots the server from the USB, allowing control of the system and access to the data that was in memory prior to the reboot • ***Removal of DIMMs:*** Attacker removes the DIMMs/NVDIMMs and steals the data • ***Direct Memory Access (DMA) attacks***: Programmable I/O devices can be put in the server to read from or write to main memory, allowing attacker to steal data
What does it do?	***Encrypts all data*** in main system memory
When should it?	***Edge computing*** or ***anywhere where physical security of the server cannot be assured.*** (Colocation facilities, factory floor, Telco closet, etc.)
What is required?	SME is enabled in BIOS. It ***does not require any changes to your OS or Applications***
What is the performance impact?	***Performance impact is negligible*** for most workloads and is <2% as measured by SPECint®_rate2006

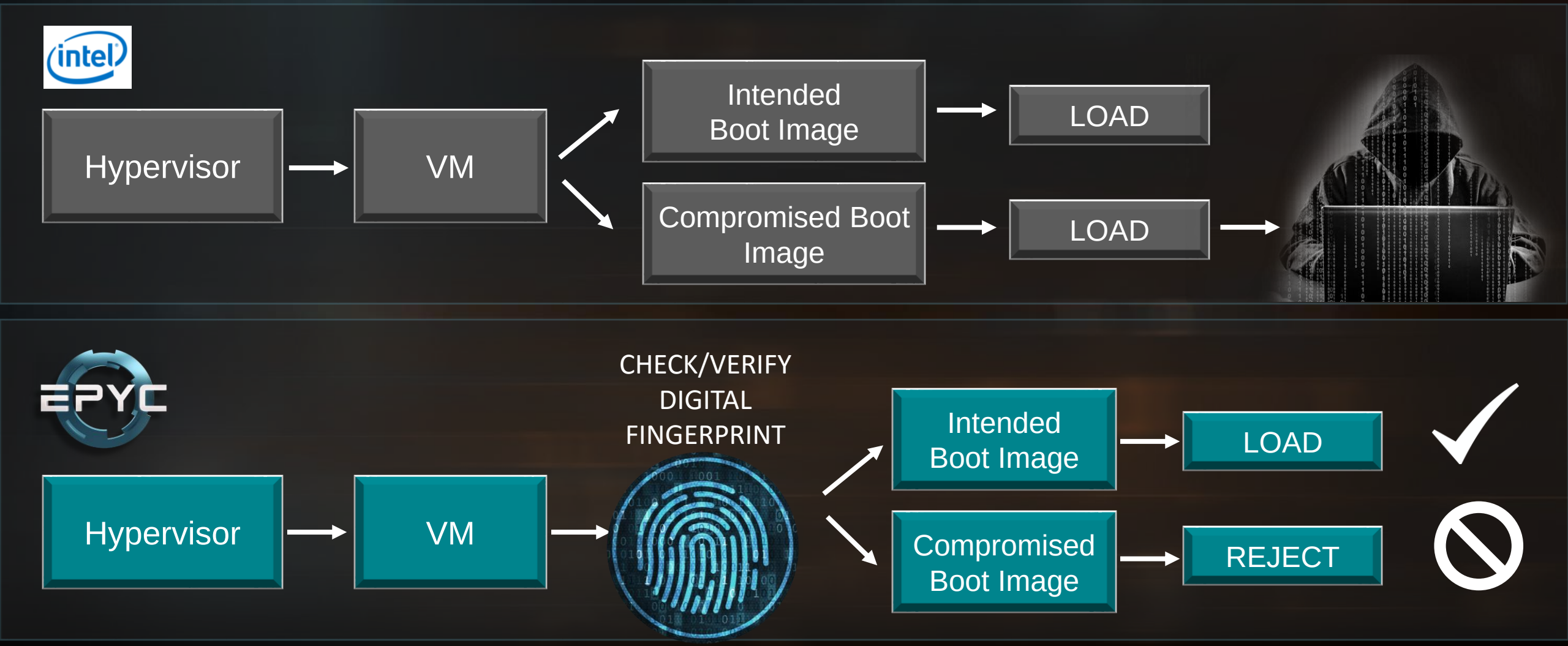
SECURE ENCRYPTED VIRTUALIZATION (SEV)

PROTECT YOUR DATA FROM INTERNAL AND EXTERNAL ATTACKS – PERFECT FOR CLOUD AND VIRTUALIZED WORKLOADS

Why do you need SEV?	• ***$7M –*** The average total organizational cost of a US data breach in 2016[1] • ***Over 40% of malicious attacks come from internal sources***[2] • **SEV protects against rouge administer attacks and break out attacks from compromised VM's**
What does SEV do?	• The Hypervisor and each Guest VM are issued unique keys which is used to encrypt main memory. This provides cryptographic ***isolation of VMs from each other and from the Hypervisor.*** • Provides VM image attestation and will not boot the VM if it has been compromised
Where to use SEV?	Cloud environments and virtualized workloads
What is required?	SEV is enabled in BIOS and the Hypervisor and each Guess OS must be SEV enabled
What is the performance impact?	AMD EPYC performance impact is negligible for most workloads. Under 2% as measured by SPECint®_rate2006

AMD Secure Root of Trust Technology - SEV

BOOT ONLY WHAT YOU AUTHORIZE AND REJECT COMPROMISED SW



End Notes

1 - Source: Ponemon Institute LLC. 2016 Cost of Data Breach Study: Global Analysis. Sponsored by IBM. www.securityintelligence.com/media/2016-cost-data-breach-study

2 - Source: IBM X-Force Research. Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations. 2016. https://securityintelligence.com/this-just-in-read-all-about-it-an-ibm-survey-of-the-threat-landscape

AMD

Thanks

For additional information visit: amd.com/epyc