AMD INFINITY GUARD AND ZERO TRUST ARCHITECTURE

WHITEPAPER | APRIL 2025

As organizations embrace cloud computing, security has become a critical concern. Cloud resources operate outside traditional network boundaries, making legacy boundary defenses like firewalls insufficient against sophisticated attacks or internal vulnerabilities.

Zero trust cloud security addresses these challenges with a multilayered approach that emphasizes never trust, always verify. It helps ensure robust protection through continuous validation and role-based authorization for users and devices.

This dynamic framework strengthens defenses against modern cyber threats while enabling organizations to confidently navigate the complexities of the cloud era.

AMD INFINITY GUARD

AMD Infinity Guard integrates several features that align closely with the Zero Trust Architecture (ZTA), a security model that assumes no entity, whether inside or outside a network, can be trusted without verification. ZTA focuses on verifying every access request, maintaining strict control, and minimizing attack surfaces. Here's how AMD Infinity Guard aligns with Zero Trust Architecture principles:

Secure Memory Encryption (SME) and Secure Encrypted Virtualization (SEV)

- **Alignment with Zero Trust:** Zero Trust models require data protection in every state—at rest, in transit, and in use. AMD Infinity Guard's SME and SEV features align with this by encrypting data in memory.
- **SME:** Defends sensitive data in system memory by encrypting it, helping ensure that attackers who gain access to physical memory cannot read the data.
- **SEV:** Provides memory encryption for virtualized environments, helping ensure that each virtual machine's (VM) memory is isolated and encrypted, defending it from other VMs and even the hypervisor.
- **Benefit to ZTA:** These encryption features support data confidentiality and isolation, even from privileged administrators or compromised components within the infrastructure, adhering to the principle of least privilege and minimizing trust within the system.

Hardware Root of Trust (Secure Boot)

- **Alignment with Zero Trust:** In Zero Trust, every device must prove its integrity before it's trusted. AMD Infinity Guard's Secure Boot feature helps to ensure the platform's trustworthiness by only allowing trusted and signed firmware and software to run during the boot process.
- Secure Boot verifies the integrity of the system firmware before the operating system starts, helping prevent malicious code from executing at the most fundamental levels.
- **Benefit to ZTA:** By verifying that only legitimate, trusted code can execute, AMD Secure Boot helps prevent compromised or malicious software from gaining a foothold in the system, aligning with ZTA's principle that no device should be trusted by default.

Shadow Stack and Control-flow Enforcement Technology (CET)

- **Alignment with Zero Trust:** Zero Trust Architecture emphasizes protecting against persistent threats and assuming breach scenarios. AMD Shadow Stack and Control-flow Enforcement Technology (CET) provide hardware-based protections against common attack vectors like buffer overflows and Return-Oriented Programming (ROP) attacks.
- **Shadow Stack:** Helps ensure that the system can detect and respond to malicious changes in the execution flow of applications, defending against control-flow hijacking attacks.
- **Benefit to ZTA:** These protections help ensure the integrity of the system, even if an attacker is able to breach parts of the system. It deters advanced persistent threats (APTs) and runtime attacks, helping keep systems resilient and trusted.

AMD Secure Processor (ASP)

- **Alignment with Zero Trust:** AMD Secure Processor (ASP) is a security co-processor that manages cryptographic keys and enforces hardware-based security policies.
- The ASP handles the generation and protection of cryptographic keys, secure boot, and firmware verification, helping ensure that sensitive operations are isolated and defended at the hardware level.
- **Benefit to ZTA:** By offloading security functions to a dedicated and isolated security processor, ASP helps ensure that trust is established and maintained at the hardware level. This helps in verifying the identity and integrity of both the platform and the software running on it.

SME (Data in Use Protection)

- **Alignment with Zero Trust**: In a Zero Trust environment, data must be always protected, including when it is being processed in memory. SME helps by encrypting sensitive data while in use, providing defense against physical memory attacks.
- **Benefit to ZTA:** It adds a layer of protection by helping ensure that attackers who manage to compromise the memory cannot access or steal sensitive data, even while it is being processed by the system. This aligns with Zero Trust principles of minimizing trust in system components and reducing the attack surface.

Firmware Trusted Platform Module (fTPM)

- **Alignment with Zero Trust:** The fTPM offers cryptographic functions such as secure key storage, attestation, and integrity checks, which are essential for establishing trust within a Zero Trust model.
- The fTPM is integrated into the platform and can securely store credentials, keys, and other sensitive information.
- **Benefit to ZTA:** This capability supports the Zero Trust goal of continuous validation of identity and device health, helping ensure that no trust is granted without verification.

SMM Supervisor Mode Execution Protection (SMEP)

- **Alignment with Zero Trust:** Zero Trust assumes that breaches can happen even in highly privileged code, such as system management mode (SMM). The AMD SMM Supervisor Mode Execution Protection (SMEP) helps prevent malicious code execution within the most privileged areas of the system.
- **Benefit to ZTA:** This hardware-based protection capability helps ensure that unauthorized code cannot execute in SMM, maintaining the integrity and security of the core operating environment even when privileged code is compromised.

Physical Attack Resistance

- **Alignment with Zero Trust:** ZTA assumes that physical access to devices is a potential attack vector. AMD Infinity Guard includes protections against physical tampering with memory or firmware.
- **Benefit to ZTA:** This reduces the trust in the physical environment and assumes attackers could have physical access to devices, aligning with Zero Trust principles that every device is vulnerable and must be protected comprehensively.

Support for Advanced Cryptography and Key Management

- **Alignment with Zero Trust:** ZTA emphasizes the use of strong encryption and secure key management to defend data and communications across untrusted networks. Infinity Guard offers hardware-based cryptography for strong encryption of data at all levels (in memory, at rest, and in use) and supports secure key management through the ASP and fTPM.
- **Benefit to ZTA:** This helps ensure that encryption keys and sensitive cryptographic operations are defended at the hardware level, reducing the chances of compromise even in a Zero Trust environment.

Continuous Verification with Integrity Measurement Architecture (IMA)

- **Alignment with Zero Trust:** ZTA requires continuous monitoring and verification of system health. AMD Infinity Guard's integration with systems like IMA (Integrity Measurement Architecture) helps ensure that the platform can continuously verify the integrity of critical components.
- **Benefit to ZTA:** This continuous monitoring fits into the Zero Trust principle of ongoing verification rather than assuming any user, device, or process can be trusted after initial authentication.

ZTA BENEFIT SUMMARY

AMD SECURITY FEATURE	BENEFIT FOR ZERO-TRUST ARCHITECTURE
SECURE MEMORY ENCRYPTION (SME) & SECURE ENCRYPTED VIRTUALIZATION (SEV)	These encryption features support data confidentiality and isolation, even from privileged administrators or compromised components within the infrastructure, adhering to the principle of least privilege and minimizing trust within the system.
HARDWARE ROOT OF TRUST (SECURE BOOT)	By helping ensure that only legitimate, trusted code can execute, AMD Secure Boot defends against compromised or malicious software gaining a foothold in the system, aligning with ZTA's principle that no device should be trusted by default.
SHADOW STACK AND CONTROL-FLOW ENFORCEMENT TECHNOLOGY (CET)	These protections help ensure the integrity of the system, even if an attacker is able to breach parts of the system. It mitigates advanced persistent threats (APTs) and runtime attacks, helping keep systems resilient and trusted
AMD SECURE PROCESSOR (ASP)	By offloading security functions to a dedicated and isolated security processor, ASP helps ensure that trust is established and maintained at the hardware level. This helps in verifying the identity and integrity of both the platform and the software running on it.
SME (DATA IN USE PROTECTION)	It adds a layer of protection by helping ensure that attackers who manage to compromise the memory cannot access or steal sensitive data, even while it is being processed by the system. This aligns with Zero Trust principles of minimizing trust in system components and reducing the attack surface.
FIRMWARE TRUSTED PLATFORM MODULE (FTPM)	This capability supports the Zero Trust goal of continuous validation of identity and device health, helping ensure that no trust is granted without verification.
SMM SUPERVISOR MODE EXECUTION PROTECTION (SMEP)	This hardware-based capability helps ensures that unauthorized code cannot execute in SMM, maintaining the integrity and security of the core operating environment even when privileged code is compromised
PHYSICAL ATTACK RESISTANCE	This reduces the trust in the physical environment and assumes attackers could have physical access to devices, aligning with Zero Trust principles that every device is vulnerable and must be protected comprehensively.
SUPPORT FOR ADVANCED CRYPTOGRAPHY AND KEY MANAGEMENT	This helps ensure that encryption keys and sensitive cryptographic operations are defended at the hardware level.
CONTINUOUS VERIFICATION WITH INTEGRITY MEASUREMENT ARCHITECTURE (IMA)	This continuous monitoring fits into the Zero Trust principle of ongoing verification rather than assuming any user, device, or process can be trusted after initial authentication.

CONCLUSION

AMD Infinity Guard aligns well with Zero Trust Architecture with its hardware-based security features including:

Root of trust authentication and attestation services support zero trust models in data centers with hardware-based security controls.

The Secure Encrypted Virtualization (SEV), the AMD technology for confidential computing, extends zero trust principles to the hypervisor so that guests no longer have to trust the hypervisor by default.

AMD hardware-based security features, including Shadow Stack and ASP, provide a strong security foundation to implement zero trust on AMD silicon.