AMD INFINITY GUARD[1]: GRUNDLAGE FÜR DIE SICHERHEIT VON IT-ÖKOSYSTEMEN IN EINER DATENGESTEUERTEN WELT

AMD
together we advance_

AMD Infinity Guard ist eine Palette an ausgeklügelten Sicherheitsfunktionen auf Systemebene, die auf eine datengesteuerte Welt ausgelegt sind. Integriert in die AMD EPYC™ Prozessoren sind die modernen Funktionen darauf ausgelegt, Daten während der Nutzung zu schützen, da diese ein zunehmend beliebtes Ziel für böswillige Akteure darstellen.

DIE CHANCE: DATENGENERIERUNG STEIGT RASANT

Daten steigern das Umsatzwachstum für viele Unternehmen und ihr Wert war noch nie so hoch. Sie treiben auch soziale Medien, KI und Anwendungen für die Zusammenarbeit voran, die unsere datengesteuerte Welt in Schwung bringen.

DAS RISIKO: BEDROHUNGEN DER DATENSICHERHEIT NEHMEN ZU – UND ENTWICKELN SICH WEITER

Hochgeschwindigkeitsnetzwerke der nächsten Generation, KI und Cloud-Computing bringen alle neue Risiken und Schwachstellen für Daten mit sich. Böswillige Akteure haben ihre Angriffe in letzter Zeit auch auf die Daten konzentriert, die in Nutzung sind und gerade von der CPU verarbeitet werden, was in der Vergangenheit oft übersehen wurde.

DIE ANTWORT: AMD INFINITY GUARD – SCHÜTZEN, ERKENNEN, VORSCHRIFTEN EINHALTEN

Integriert auf Chip-Ebene macht AMD Infinity Guard Serversysteme zu einer Grundlage für Unternehmens- und Cloud-Sicherheitsfunktionen in einer datengesteuerten Welt. Die modernen Funktionen tragen dazu bei, Schutzschichten um die Daten herum zu bilden, um interne und externe Bedrohungen abzuschwächen und sie zu Compliance-Zwecken nachzuverfolgen.

3 ARTEN, AUF DIE AMD INFINITY GUARD IHRE DATEN SCHÜTZT

1 CONFIDENTIAL COMPUTING

Technologien zur sicheren verschlüsselten Virtualisierung (SVV) helfen, Daten während der Verarbeitung zu schützen – selbst Cloud-Serviceanbieter haben keinen Zugriff. Dies ist die Grundlage des Confidential Computing – nur die Person oder der Dienst, der die Daten „besitzt", kann sie entschlüsseln.

2 SCHIRMT DEN SYSTEMSPEICHER GEGEN AUSSPÄHEN AB, SELBST IN DER CLOUD

Sicherheitsbedrohungen von innerhalb der Organisation sind ein großes Risiko. Sichere Speicherverschlüsselung (SSV) schützt bei Angriffen auf die Integrität des Hauptspeichers vom Bare Metal bis in die Cloud, z. B. bestimmte Kaltstartangriffe.

3 BOOTET NUR, WAS GEBOOTET WERDEN SOLL

AMD Secure Boot ist so konzipiert, dass nur autorisierte Firmware gebootet werden kann. Mit dieser Defense-in-Depth-Funktion soll eine starke Verteidigung bei zunehmenden Angriffen auf Firmwareebene bereitgestellt werden.

MEHR ERFAHREN ÜBER AMD INFINITY GUARD

Mehr erfahren

1. Die Funktionen von AMD Infinity Guard variieren je nach EPYC™ Prozessorgeneration. Sicherheitsfunktionen von Infinity Guard müssen von Server-OEMs und/oder Cloud-Dienstanbietern vor Betrieb aktiviert werden. Wenden Sie sich an Ihren OEM oder Anbieter, um die Unterstützung dieser Funktionen zu bestätigen. Mehr erfahren über Infinity Guard unter https://www.amd.com/de/technologies/infinity-guard. GD-183

AMD
together we advance_data centers