DELL Technologies

AMD
together we advance_

Documento técnico

Protección de la frontera digital: Enfoque de confianza cero de Inside Dell y AMD

Proteja su organización con la seguridad integral de Dell y AMD

Tabla de contenido

Introducción

Los dispositivos que nos conectan hacen posibles cosas increíbles, pero estas conexiones también pueden ofrecer puntos adicionales de vulnerabilidad que los actores maliciosos pueden aprovechar. De hecho, algunas estimaciones predicen que los ciberataques costarán a las organizaciones 10,5 billones de dólares en 2025.[1] Y según una estimación, recuperarse de los daños de un ciberataque puede llevar aproximadamente 277 días.[2]

Aunque las nuevas tecnologías, como la inteligencia artificial (IA), ofrecen mejoras en la productividad y las operaciones empresariales a muchas organizaciones, también hacen que los datos sean vulnerables a ciberataques más sofisticados. Con cada avance tecnológico, los líderes de este sector deben cambiar las estrategias para contrarrestar de forma eficaz a los ciberdelincuentes que encuentran nuevas formas de conseguir y aprovechar los datos. Para frustrar estas amenazas y mantener los datos a salvo, todos los componentes del centro de datos, desde los servidores y el almacenamiento hasta las redes, el software y el firmware, deben contar con protección integrada. La protección comienza con la mitigación de las manipulaciones de la cadena de suministro en la planta de fabricación y continúa con el proceso de transporte y el uso por parte del cliente. Y los ataques ya no se reducen a las paredes del centro de datos. Las organizaciones con presencia en la cloud se enfrentan a desafíos adicionales para mantener los datos protegidos.

Juntos, Dell y AMD proporcionan una arquitectura ciberresiliente diseñada a medida que ayuda a las organizaciones a adoptar una estrategia de confianza cero, adoptando la idea de que los componentes del sistema son vulnerables en cada eslabón de la cadena y ofreciendo protección en todos los puntos. Una estrategia de confianza cero utiliza sólidas políticas basadas en la identidad para cada activo de TI, junto con principios de "mínimos privilegios" para el acceso. La arquitectura ciberresiliente de Dell incluye características exhaustivas centradas en la integridad del arranque y la protección de datos, además de características de seguridad en Integrated Dell Remote Access Controller (iDRAC). Los servidores Dell PowerEdge se anclan con una raíz de confianza (RoT) basada en chip que establece una cadena de confianza para la verificación criptográfica de los componentes de hardware y software del servidor. AMD Infinity Guard proporciona una capa de seguridad adicional que reduce el potencial de ataque durante el arranque y la ejecución del software. AMD Infinity Guard incorpora varias características de seguridad adicionales, como Platform Secure Boot y Platform Secure Processor, que garantizan que los servidores PowerEdge estén protegidos en cada etapa de su ciclo de vida.

Arquitectura ciberresiliente de Dell

La arquitectura ciberresiliente de Dell utiliza las características de seguridad de PowerEdge, que trabajan en conjunto para ofrecer resiliencia y permitir una estrategia de confianza cero. Las características de seguridad deben proteger contra las posibles amenazas, detectar actividades sospechosas y permitir una recuperación rápida en caso de vulneración. Al mismo tiempo, también deben mantener una postura de "verificar antes de confiar" para un enfoque de confianza cero de mínimos privilegios, en el que los usuarios y dispositivos solo pueden acceder a lo que necesitan para realizar sus tareas. Trabajando juntos, estos controles de seguridad de PowerEdge ofrecen una solución de seguridad completa que garantiza la resiliencia, a la vez que impone una postura de confianza cero. Para obtener más información sobre todas las características de la arquitectura ciberresiliente de Dell y los servicios, consulte el documento técnico.

Garantía de integridad del arranque

El entorno previo al arranque suele pasarse por alto y, si no se toman medidas de protección, puede estar expuesto a un ataque. Si un actor malicioso pone en riesgo el BIOS, el firmware o un controlador durante el arranque, es posible que pueda tener acceso a todo el sistema. Sin los controles adecuados, podría infiltrarse con éxito en el sistema en cualquier punto y llegar hasta el objetivo deseado: sus datos.

Para mitigar las vulnerabilidades, el proveedor de servidores debe proteger el BIOS, pero también verificar y validar los componentes específicos de los servidores y el firmware, como la memoria y los procesadores. Los fabricantes de hardware de servidor deben asegurarse de que sus componentes se integren completamente en la arquitectura de servidor para que las comprobaciones de seguridad y validación funcionen de forma óptima. Todos los servidores Dell PowerEdge ofrecen varias capas de seguridad para proteger el ciclo de arranque: una RoT basada en chip, arranque seguro de UEFI y características de seguridad de iDRAC, que incluyen reversión de firmware y recuperación rápida del sistema operativo.

Además de estas capas de seguridad basadas en los servidores Dell PowerEdge, los procesadores AMD cuentan con Platform Secure Boot (PSB) y Platform Security Processor (PSP) para proteger los datos en uso. Juntos, Dell y AMD cubren todos los aspectos del ciclo de arranque para garantizar una base segura para sus datos y cargas de trabajo.

[1] Chuck Brooks, "Cybersecurity Trends & Statistics For 2023; What You Need to Know", acceso el 4 de diciembre de 2023, https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=9885ce219dba.

[2] Ken Kizzee, "Cyber Attack Statistics to Know", acceso el 19 de diciembre de 2023, https://parachute.cloud/cyber-attack-statistics-data-and-trends/.

iDRAC y raíz de confianza de Dell

El concepto de RoT asume que, si un sistema verifica una base o referencia como segura, todas las validaciones y comprobaciones de seguridad posteriores quedarán ancladas en una cadena de confianza continua. Imaginemos una casa: si los cimientos son inestables y empiezan a desmoronarse, la integridad de las paredes importa poco. Del mismo modo, si el BIOS se ve en riesgo, proteger el sistema operativo del servidor puede ser en vano.

La cadena de confianza de los servidores PowerEdge ofrece una verificación criptográfica optimizada en todos los componentes del servidor, desde los cimientos hasta los datos. Esto garantiza que los componentes de la pila de software del sistema (hipervisor, sistema operativo y aplicaciones) sepan que pueden confiar en el servidor subyacente cuando este está operativo. Esta capa establece las bases de la cadena de confianza dentro de un servidor y crea una plataforma de servidor segura y de confianza. Para la verificación criptográfica, los servidores Dell utilizan una exclusiva RoT basada en chip en cada servidor, lo que garantiza un arranque seguro en cada arranque en frío o ciclo de encendido de CA. A partir de la versión 4.10.10.10, iDRAC ofrece un mecanismo de RoT para verificar la imagen del BIOS en el arranque y no permitir que el servidor se inicie hasta que se verifique la imagen del BIOS. En el caso de los servidores PowerEdge con procesadores AMD, Integrated Dell Remote Access Controller (iDRAC) aprovecha la tecnología PSB de AMD para verificar el código del BIOS antes de cargar el sistema operativo. AMD PSB examina la integridad del BIOS, actuando como interfaz entre la ROM del BIOS primario y AMD Fusion Controller Hub (FCH) para un procesamiento de la RoT completo. Esta validación meticulosa se extiende al cargador de arranque del sistema operativo, garantizando una cadena de confianza continua.

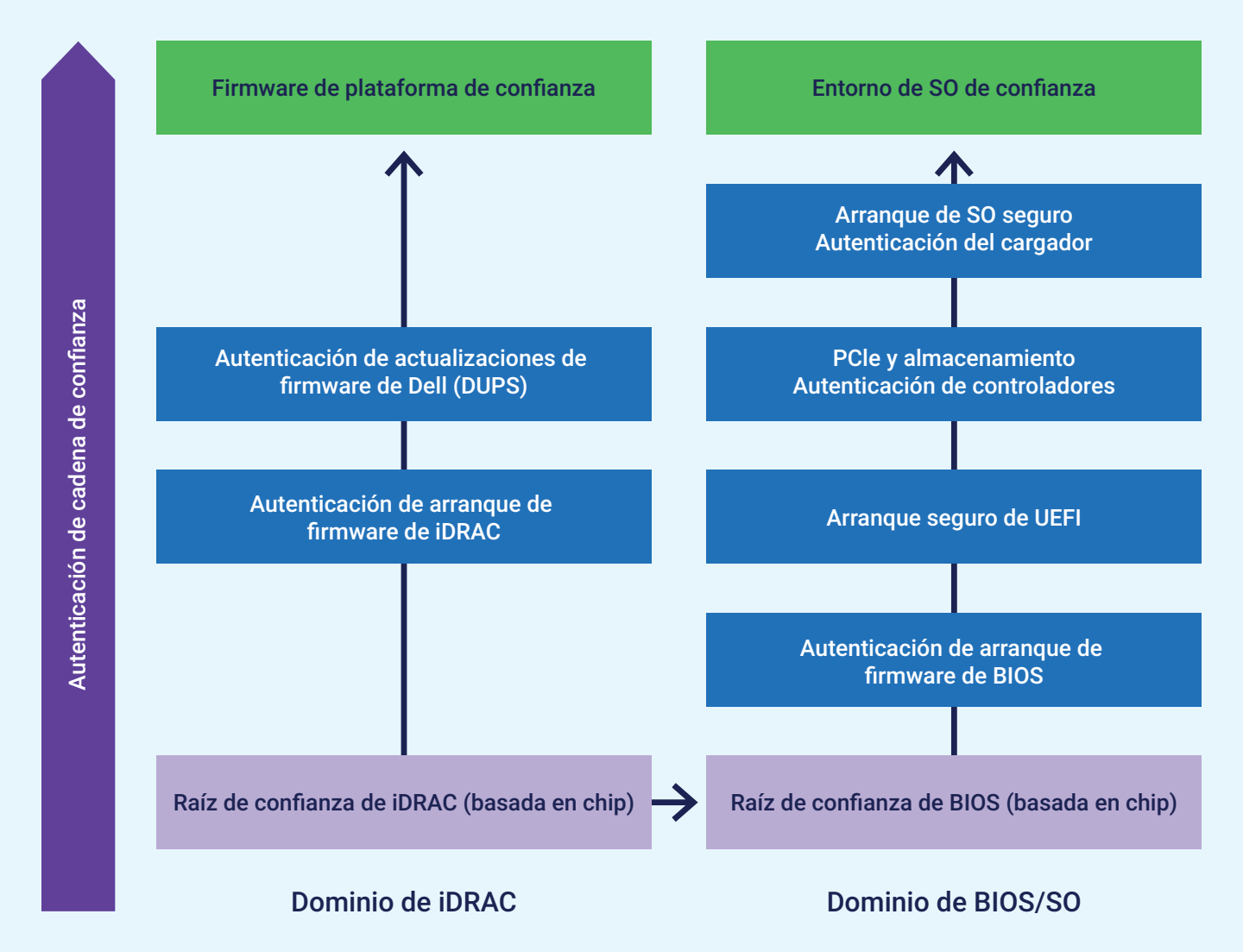

Figura 1: Dominios de raíz de confianza basada en chip en servidores PowerEdge con iDRAC9.

Si falla la validación del BIOS, iDRAC apaga inmediatamente el servidor y notifica al usuario, evitando el arranque de firmware no autorizado. iDRAC también incluye un sistema de copia de seguridad y recuperación para el BIOS y el firmware de iDRAC, que refuerza la fiabilidad del servidor y protege las operaciones del servidor contra la posible corrupción del firmware. Para proporcionar protección adicional, iDRAC también ofrece un análisis del BIOS en directo que los usuarios pueden ejecutar bajo demanda o ejecutar de forma regular mediante un programa. Este análisis requiere la licencia de iDRAC Datacenter y permite a los usuarios detectar posibles problemas antes del reinicio, lo que permite una mitigación proactiva.[3]

Arranque seguro de UEFI

Los servidores Dell PowerEdge utilizan el arranque seguro de UEFI estándar del sector para validar los cargadores de arranque específicos del sistema operativo, garantizando la integridad del kernel del sistema operativo y otros componentes críticos. UEFI actúa como protección frente al malware y el ransomware en entornos previos al arranque. Para garantizar la interoperabilidad, los fabricantes de servidores y componentes deben colaborar para asegurarse de que el BIOS habilitado por UEFI reconozca las firmas de los controladores y el firmware para los componentes. Mediante la validación de las firmas criptográficas de los controladores UEFI y otro código previo al sistema operativo, el arranque seguro de UEFI se encarga de garantizar que todo el código cargado durante el arranque esté libre de contenido malicioso.

Para aumentar la personalización de la seguridad, los administradores pueden configurar certificados de firma personalizados del cargador de arranque del sistema operativo para el arranque seguro de UEFI. (Para obtener más información acerca de la personalización del arranque seguro de UEFI, visite https://infohub.delltechnologies.com/section-assets/direct-from-development-uefi-boot-enhanced-security-to-combat-threats). Esto restringe la ejecución a los cargadores de arranque seguros y de confianza del sistema operativo, lo que permite una cadena de arranque segura mediante la autenticación del kernel del sistema operativo y el sistema de archivos. Esta característica ofrece flexibilidad adicional, especialmente para los administradores de Linux que prefieren firmar sus propios cargadores de arranque del sistema operativo, en lugar de depender de autoridades de certificados UEFI predeterminadas de terceros. Los administradores pueden cargar certificados personalizados a través de la API de iDRAC, lo que mejora la autenticación de sus cargadores de arranque del sistema operativo específicos. De manera excepcional, los servidores Dell PowerEdge admiten la personalización completa del arranque seguro, lo que incluye la opción de eliminar todos los certificados estándar de Microsoft, VMware o la autoridad de certificados UEFI.[4]

Validación de CPLD

Todos los servidores Dell PowerEdge validan el dispositivo lógico programable complejo (CPLD) en cada arranque de CA. CPLD, un versátil dispositivo lógico programable,[5] se compone de varios PLD individuales conectados a una matriz de conmutación programable. Su firmware, normalmente almacenado en la EEPROM, la memoria flash o la SRAM, permite realizar modificaciones en las funciones de la placa base más allá de las capacidades del BIOS, lo que incluye la implementación de lógica específica para las interacciones de los dispositivos con la placa base. La validación de CPLD garantiza que las modificaciones de la placa base no dañen los servidores o sus datos.

Seguridad de hardware de iDRAC

Para ampliar la cadena de confianza a componentes de hardware adicionales, iDRAC utiliza el modelo de datos del protocolo de seguridad (SPDM), que estandariza la forma en la que los servidores recopilan la información sobre sus componentes. La identidad, el firmware y la información de configuración de cada componente se cifran. La seguridad de hardware de iDRAC utiliza intercambios de claves autenticadas para proteger las líneas de comunicación entre los componentes e iDRAC. Con SPDM, iDRAC puede autenticar la validez de los componentes, como los controladores RAID PowerEdge (PERC)12 y las tarjetas de interfaz de red (NIC), lo que no solo mejora la seguridad del servidor mediante la autenticación de los certificados de identidad del dispositivo de los componentes, sino que también alerta a los usuarios de cualquier fallo de autenticación.

[3] Dell, "Improved security with iDRAC9 using Root of Trust and BIOS Live Scanning", acceso el 19 de diciembre de 2023, https://dl.dell.com/manuals/common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf.

[4] Dell, "Cyber Resilient Security in Dell PowerEdge Servers", acceso el 4 de diciembre de 2023, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/cyber-resilient-security-with-poweredge-servers.pdf.

[5] Technopedia, "Complex Programmable Logic Device", acceso el 4 de diciembre de 2023, https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld.

AMD Platform Secure Boot

Los procesadores AMD cuentan con AMD Platform Secure Boot (PSB) para ayudar a contrarrestar otra creciente preocupación en el panorama digital actual: las amenazas de nivel de firmware. PSB utiliza la RoT basada en chip de AMD y verifica el proceso de arranque desde el código del BIOS hasta el cargador de arranque del sistema operativo y el arranque seguro de UEFI.[6] Dell utiliza placas base habilitadas por AMD PSB para permitir que se ejecute únicamente su código del BIOS firmado criptográficamente. Además, Dell vincula cada procesador AMD con una placa base específica con fusibles programables una sola vez que enlazan el procesador con las claves de firma de código de firmware de Dell.[7] Para proteger contra los ataques destinados a incrustar malware en el firmware, los arranques de PSB autorizan solo el firmware autenticado mediante AMD Secure Processor.[8]

Mediante la verificación criptográfica de la pila de software, AMD Platform Secure Boot aporta una importante capa de defensa contra las intrusiones no autorizadas en varias plataformas, especialmente en entornos virtualizados o en la cloud.

AMD Platform Secure Processor

Junto con PSB, AMD Platform Secure Processor (PSP) refuerza el proceso de arranque de los servidores Dell PowerEdge. Cuando una CPU se enciende por primera vez en la fábrica de Dell, AMD Platform Secure Processor incrusta un ID de Dell único de forma permanente en la CPU. Este ID enlaza de forma eficaz la CPU al servidor PowerEdge, creando un vínculo seguro.[9]

Esta integración supone que PSP evitará que un servidor PowerEdge se inicie si se detecta una CPU de un servidor diferente. Sin embargo, la portabilidad de la CPU sigue siendo posible en caso de un fallo de hardware. El procesador AMD se bloquea en la clave de firma del proveedor, en lugar de en la placa base, lo que ofrece un equilibrio entre la seguridad y la movilidad de los componentes.[10]

Figura 2: Estados de los datos

[6] AMD, "AMD Pro Security", acceso el 4 de diciembre de 2023, https://www.amd.com/en/technologies/pro-security.
[7] AMD, "AMD Infinity Guard", acceso el 4 de diciembre de 2023, https://www.amd.com/en/technologies/infinity-guard.
[8] AMD, "4 Ways AMD Infinity Guard Helps Protect Your Data", acceso el 4 de diciembre de 2023, https://www.amd.com/system/files/documents/content-security-infographic.pdf.
[9] AMD, "AMD Infinity Guard".
[10] Dell, "Defense in-depth: Comprehensive Security on PowerEdge AMD EPYC Generation 2 (Rome) Servers", acceso el 4 de diciembre de 2023, https://infohub.delltechnologies.com/p/defense-in-depth-comprehensive-security-on-poweredge-amd-epyc-generation-2-rome-servers/.

Protección de los datos

Cuando los atacantes pueden acceder a los sistemas, el objetivo final siempre es el mismo: encontrar sus datos y robarlos, manipularlos, venderlos o destruirlos. El servidor físico no es el único punto de vulnerabilidad. Los actores maliciosos pueden atacar las redes, las políticas de TI pueden contener errores, los usuarios finales pueden tener contraseñas débiles y los equipos de TI pueden establecer permisos de acceso demasiado amplios. Los atacantes pueden dirigirse a los usuarios con correos electrónicos de phishing para distribuir malware.

Dell permite a los clientes implementar un enfoque de confianza cero que utiliza varias capas de seguridad para ayudar a proteger contra todos estos tipos de vulnerabilidades. Para protegerse de los robos y los riesgos, debe proteger los datos en reposo, los datos en proceso y los datos en transferencia a través de la retirada de los datos.[11] Con características como el cifrado en reposo, la sólida gestión de claves de cifrado y la renovación de certificados automatizada, los servidores Dell PowerEdge trabajan para bloquear, impedir y mitigar los ataques maliciosos después del primer arranque. Los servidores Dell PowerEdge con procesadores AMD ofrecen características adicionales para reforzar la seguridad, como AMD Secure Memory Encryption (SME) y Secure Encrypted Virtualization (SEV).

Datos en reposo

Para proteger los datos en reposo, Dell ofrece tres características de seguridad principales: cifrado basado en software, gestión de claves de cifrado y cifrado de unidades de hardware. Con las unidades compatibles con Instant Secure Erase (ISE), los clientes de Dell pueden borrar criptográficamente los datos de unidades de cifrado automático (SED), unidades ISE y dispositivos NVM, como NVDIMM. Las SED protegen los datos de los ataques en caso de que un empleado insatisfecho u otro actor malicioso extraiga físicamente las unidades de un servidor. Debido a que la contraseña de la clave de bloqueo de la unidad cifrada la vincula a un servidor específico y al controlador RAID del que provenía, otro servidor no puede acceder a los datos. Para mayor protección, iDRAC utiliza Dell OpenManage Secure Enterprise Key Manager con gestión de claves local (iLKM, LKM), que trabaja junto con un gestor de claves externo para bloquear y desbloquear el controlador de almacenamiento en el arranque. Si alguien arranca el servidor fuera del gestor de claves, iDRAC mantiene el controlador de almacenamiento bloqueado para que los datos almacenados en el dispositivo sigan cifrados. Para obtener más información sobre otras opciones de clave de cifrado, visite https://infohub.delltechnologies.com/section-assets/openmanage-sekm-storage-performance-infographic.

Datos en transferencia

Con los datos en transferencia, las vulnerabilidades en la red y el control de acceso a los datos podrían permitir que los atacantes intercepten o modifiquen los datos que viajan por la red. La conexión web de iDRAC es un posible punto de vulnerabilidad, por lo que Dell ofrece varias opciones para proteger la conexión con un certificado TLS/SSL, mitigando así la posibilidad de ataque. Aunque este certificado está autofirmado de forma predeterminada, los administradores pueden crear un certificado personalizado o uno firmado por una autoridad de certificación (CA) de confianza. Este certificado permite conexiones cifradas y seguras para navegadores web y herramientas como utilidades de línea de comandos para interactuar de forma segura con el servidor a través de la conexión de iDRAC.

iDRAC también ofrece varios controles para que los usuarios modifiquen las estrictas reglas de acceso que permiten a SSH acceder al servidor. Para los usuarios de iDRAC con una licencia de nivel de Datacenter, iDRAC ofrece Simple Certificate Enrollment Protocol (SCEP), que mantiene los certificados del servidor web con renovación automática para evitar lapsos de cobertura accidentales. Un estudio de 2020 de Principled Technologies determinó que esta función de renovación automática mantiene los servidores más protegidos, a la vez que ahorra un valioso tiempo al personal de TI, especialmente en el mantenimiento de una flota de certificados de servidor.[12]

Datos en uso

Para proteger los datos en uso, los servidores Dell PowerEdge cuentan con funciones de computación confidenciales de AMD, que incluyen AMD Secure Memory Encryption (SME) y Secure Encrypted Virtualization (SEV) para proteger los datos mientras viajan por los componentes de memoria y procesamiento.

[11] Dell, "Reduce Your Risk of Unauthorized Server Data Access", acceso el 24 de enero de 2024, https://infohub.delltechnologies.com/section-assets/data-protection-infographic.

[12] Principled Technologies, "Reduce hands-on deployment times to near zero with iDRAC9 automation", acceso el 4 de diciembre de 2023, https://www.principledtechnologies.com/Dell/iDRAC9-v6.10-provisioning-infographic-0323.pdf.

Secure Memory Encryption

AMD SME cifra todos los datos cuando entran en la memoria, lo que aumenta la protección de estos. Sin cifrado de memoria, los datos son vulnerables al software malicioso y otras intrusiones, especialmente con la tecnología de memoria más reciente, como NVDIMM, que no pierde los datos en el encendido. Esta protección se extiende a la memoria a través de motores de cifrado de alto rendimiento integrados en los canales de memoria, lo que garantiza la seguridad y velocidad. Debido a que es totalmente transparente para el sistema operativo host y las capas de aplicaciones, AMD SME consigue hacer esto sin necesidad de cambios en el software de aplicación, lo que ofrece un enfoque sencillo para mejorar la seguridad de la memoria.[13]

El cifrado de datos en memoria de AMD SME supone un cambio en relación con los métodos de cifrado de memoria anteriores, que se personalizaban para casos de uso específicos. Una ventaja clave de AMD SME es su flexibilidad, ya que permite su uso por parte del software de formas diferentes: mediante el cifrado de toda la DRAM para una protección completa o mediante el cifrado selectivo de regiones específicas, como las que utilizan las máquinas virtuales (VM) invitadas.[14]

AMD Secure Encrypted Virtualization

AMD SEV mejora el cifrado de la memoria y las máquinas virtuales mediante la implementación de un Trusted Execution Environment (TEE) basado en máquina virtual. Al integrarse con la arquitectura AMD-V, AMD SEV cifra la memoria de cada VM por separado, protegiendo las VM una de otra y del hipervisor. Este enfoque emplea criptografía para proteger el código dentro de una VM frente a códigos con mayores privilegios potencialmente vulnerables, como el hipervisor. La capa adicional de seguridad es especialmente crucial en entornos de cloud. Este método garantiza una protección mejorada de las VM, reforzándolas contra las vulnerabilidades externas. El cifrado se produce en el controlador de memoria, donde se cifran y descifran los datos sin ralentizar la velocidad de procesamiento, gracias a que AMD Secure Processor gestiona todos los detalles del cifrado de forma invisible.[15]

Todavía existen soluciones en las que los datos de las VM deben comunicarse con otras VM o con el hipervisor. En esos casos, AMD SEV permite a la VM elegir qué clave de cifrado se aplica a páginas de la memoria específicas: una clave de invitado que mantiene la privacidad de la página para la VM o una clave de hipervisor que permite a este y a otras VM descifrar la página. Esta flexibilidad permite la seguridad y la comunicación basadas en las necesidades de cada VM.[16]

AMD SEV ofrece características adicionales que amplían el aislamiento criptográfico de las VM: SEV-Encrypted State (SEV-ES) y SEV-Secure Nested Paging (SEV-SNP). SEV-ES aísla aún más las VM y el hipervisor entre sí cifrando el contenido de registro de la CPU cuando una VM se enciende, protegiéndola del acceso no autorizado a través de una VM vecina o del hipervisor. SEV-SNP se basa en SEV y SEV-ES, y añade protección de integridad de la memoria y características de seguridad adicionales opcionales para las VM. La mejora de la integridad de la memoria permite que una VM pueda acceder a los datos de la memoria solo si puede leer el último valor que se ha escrito. Si otra entidad ha modificado los datos de la memoria, la VM no puede acceder a estos. Esto protege la VM de la ejecución de datos o código en riesgo.

Cifrado y claves de cifrado

AMD SEV utiliza una clave de cifrado única para cada VM, aislando criptográficamente las VM y el hipervisor. Este motor de cifrado protege los datos en la escritura y los descifra en la lectura. Cada VM, en su creación, recibe una clave única, lo que garantiza que cualquier intento no autorizado de acceder a su memoria genere datos incomprensibles. Todos los procesadores AMD EPYC™ de 4.ª generación ofrecen hasta mil claves de cifrado. Esta arquitectura no altera las aplicaciones dentro de la VM, opera en el nivel del sistema operativo y aumenta la seguridad de los datos. Diseñado para proteger los datos en uso, incluidos los contenidos de la memoria, el hardware de cifrado integrado en el controlador de memoria gestiona el cifrado y descifrado del tráfico de la VRAM, reforzando la protección de los datos en uso.[17]

[13] AMD, "AMD Infinity Guard".
[14] AMD, "AMD Memory Encryption", acceso el 4 de diciembre de 2023, https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf.
[15] AMD, "AMD Secure Encrypted Virtualization", acceso el 4 de diciembre de 2023, https://www.amd.com/en/developer/sev.html
[16] AMD, "AMD Memory Encryption". https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf
[17] AMD, "AMD Secure Encrypted Virtualization".

Conclusión

Desde el momento en el que solicita los servidores Dell PowerEdge con procesadores AMD hasta cuando los retira y durante todo ese tiempo, Dell y AMD ofrecen numerosas capas de seguridad para mantener sus datos a salvo. Gracias a las capas firmemente integradas de la RoT basada en chip y a las múltiples capas de protección del arranque para deshacerse de los controladores sospechosos, el firmware, las versiones del BIOS y los componentes del servidor se protegen desde el momento de la fabricación. Además, mediante el cifrado de las unidades SED e ISE, los datos están protegidos incluso si actores maliciosos extraen físicamente los discos de su centro de datos. Gracias a otras características de seguridad, como las tecnologías AMD SME y SEV basadas en procesador, que protegen los datos en proceso, y las vanguardistas comprobaciones del software a través de iDRAC, los servidores Dell PowerEdge con procesadores AMD ayudan a garantizar la continuidad empresarial sin problemas, sin importar qué nuevos métodos de ataque utilicen los ciberdelincuentes. Para obtener más información acerca de los servidores Dell PowerEdge con procesadores AMD EPYC de 4.ª generación, visite www.dell.com/servers/amd.

Más información sobre las soluciones de Dell y AMD

Póngase en contacto con un experto de Dell Technologies.

Consulte más recursos.

Únase a la conversación con #PowerEdge

DELL Technologies

AMD together we advance_