DELL Technologies

AMD
together we advance_

White paper

Mettere in sicurezza la frontiera digitale: l'approccio Zero Trust di Dell e AMD

Proteggi la tua organizzazione con la sicurezza end-to-end di Dell e AMD

Sommario

Introduzione

I dispositivi che ci connettono rendono possibili cose incredibili, ma queste connessioni offrono anche punti di vulnerabilità aggiuntivi che i malintenzionati possono sfruttare. Secondo alcune stime, infatti, entro il 2025 gli attacchi informatici costeranno alle organizzazioni fino a 10,5 trilioni di dollari.[1] Secondo una stima, il ripristino dai danni di un attacco informatico richiede circa 277 giorni. [2]

Sebbene le tecnologie più recenti, come l'intelligenza artificiale (AI), offrano miglioramenti nella produttività e nelle operazioni aziendali per molte organizzazioni, lasciano anche i dati esposti ad attacchi informatici più sofisticati. Con ogni progresso tecnologico, i leader del settore tecnologico devono cambiare strategia per contrastare efficacemente i criminali informatici che cercano nuovi modi per impossessarsi dei dati e sfruttarli. Per contrastare queste minacce e mantenere i dati al sicuro, ogni componente del data center, dai server e dallo storage alle reti, al software e al firmware, necessita di una protezione integrata. La protezione inizia con l'attenuazione delle manomissioni della supply chain nel reparto di produzione e continua per tutto il processo di trasporto e l'utilizzo da parte del cliente. E gli attacchi non si fermano più alle mura del data center. Le organizzazioni con una presenza nel cloud devono affrontare ulteriori sfide per garantire la sicurezza dei dati.

Insieme, Dell e AMD forniscono un'architettura resiliente agli attacchi informatici appositamente progettata che aiuta le organizzazioni ad adottare una strategia Zero Trust, considerando i componenti di sistema vulnerabili in ogni anello della catena e offrendo protezione in ogni punto. La strategia Zero Trust utilizza solide policy basate sull'identità per ogni risorsa IT insieme a principi di "privilegio minimo" per l'accesso. L'architettura resiliente agli attacchi informatici di Dell include funzionalità approfondite incentrate sull'integrità di avvio e sulla protezione dei dati, nonché funzionalità di protezione in iDRAC (Integrated Dell Remote Access Controller). I server Dell PowerEdge sono ancorati a una Silicon Root of Trust che definisce una catena di affidabilità per la verifica crittografica dei componenti hardware e software sul server. AMD Infinity Guard fornisce un ulteriore livello di sicurezza che riduce la potenziale area di attacco in fase di avvio ed esecuzione dati del software. AMD Infinity Guard include diverse funzionalità di sicurezza aggiuntive, tra cui Platform Secure Boot e Platform Secure Processor, che garantiscono la protezione dei server PowerEdge in ogni fase del ciclo di vita.

Architettura Dell resiliente agli attacchi informatici

L'architettura Dell resiliente agli attacchi informatici utilizza le funzionalità di protezione PowerEdge che operano in sinergia per fornire resilienza e consentire una strategia Zero Trust. Le funzionalità di protezione devono salvaguardare da potenziali minacce, rilevare attività sospette e ripartire rapidamente in caso di violazione. Allo stesso tempo, devono anche mantenere una condizione di "verifica prima di considerare attendibile" per un approccio Zero Trust dei privilegi minimi, in cui gli utenti e i dispositivi possono accedere solo allo stretto necessario per svolgere le loro attività. Interagendo, questi controlli di sicurezza di PowerEdge offrono una soluzione completa per la sicurezza che garantisce la resilienza applicando al contempo un approccio Zero Trust. Per ulteriori informazioni sulle tutte le funzionalità dell'architettura resiliente agli attacchi informatici di Dell e sui relativi servizi, consultare il white paper.

Garantire l'integrità dell'avvio

L'ambiente di pre-avvio viene spesso trascurato e, se non vengono prese misure di sicurezza, può rimanere esposto agli attacchi. Se un malintenzionato compromette il BIOS, il firmware o un driver durante l'avvio, potenzialmente può accedere all'intero sistema. Senza i controlli appropriati, può riuscire a infiltrarsi nel sistema in qualsiasi punto e raggiungere l'obiettivo desiderato: i tuoi dati.

Per ridurre le vulnerabilità, il fornitore del server deve proteggere il BIOS, ma anche verificare e convalidare componenti e firmware specifici del server, come memoria e processori. I produttori di hardware dei server devono assicurarsi che i loro componenti si integrino completamente con l'architettura del server affinché i controlli di sicurezza e convalida funzionino senza problemi. Ogni server Dell PowerEdge offre più livelli di sicurezza per proteggere il ciclo di avvio: Silicon Root of Trust, UEFI Secure Boot e funzionalità di protezione iDRAC, tra cui il rollback del firmware e il ripristino rapido del sistema operativo.

Oltre a questi livelli di sicurezza basati su server Dell PowerEdge, i processori AMD includono Platform Secure Boot (PSB) e Platform Security Processor (PSP) per proteggere i dati in uso. Insieme, Dell e AMD coprono ogni aspetto del ciclo di avvio per garantire una base sicura per i dati e i carichi di lavoro.

[1] Chuck Brooks, “Cybersecurity Trends & Statistics For 2023; What You Need to Know,” consultato il 4 dicembre 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", consultato il 19 dicembre 2023, https://parachute.cloud/cyber-attack-statistics-data-and-trends/.

Dell iDRAC e Root of Trust

Il concetto di Root of Trust presuppone che se un sistema verifica che una base o una baseline è sicura, tutte le convalide e i controlli di sicurezza successivi sono ancorati in una catena di attendibilità continua. Immagina una casa: se le fondamenta sono instabili e iniziano a sgretolarsi, l'integrità del supporto delle mura ha poca importanza. Analogamente, se il BIOS del server è compromesso, la protezione del sistema operativo del server può essere inutile.

La catena di affidabilità del server PowerEdge fornisce una verifica crittografica senza soluzione di continuità per tutti i componenti del server, dalle fondamenta ai dati. Questo garantisce che i componenti dello stack software del sistema (hypervisor, OS, applicazioni) sappiano che possono considerare affidabile il server sottostante quando è operativo. Questo livello stabilisce le basi per una catena di affidabilità all'interno del server e crea una piattaforma di server affidabile e protetta. I server Dell utilizzano un'esclusiva Silicon Root of Trust integrata in ogni server per la verifica crittografica che garantisce l'avvio sicuro a ogni avvio a freddo o ciclo di CA. A partire dalla versione 4.10.10.10, iDRAC fornisce un meccanismo di Root of Trust per verificare l'immagine del BIOS all'avvio e non consente l'avvio del server fino a quando non verifica l'immagine del BIOS. Per i server PowerEdge con processori AMD, l'iDRAC (integrated Dell Remote Access Controller) sfrutta la tecnologia AMD PSB per verificare il codice del BIOS prima del caricamento del sistema operativo. AMD PSB esamina l'integrità del BIOS, interfacciandosi con la ROM del BIOS principale e AMD Fusion Controller Hub (FCH) per un'elaborazione approfondita della Root of Trust. Questa meticolosa convalida si estende fino al bootloader del sistema operativo, garantendo una catena di affidabilità continua.

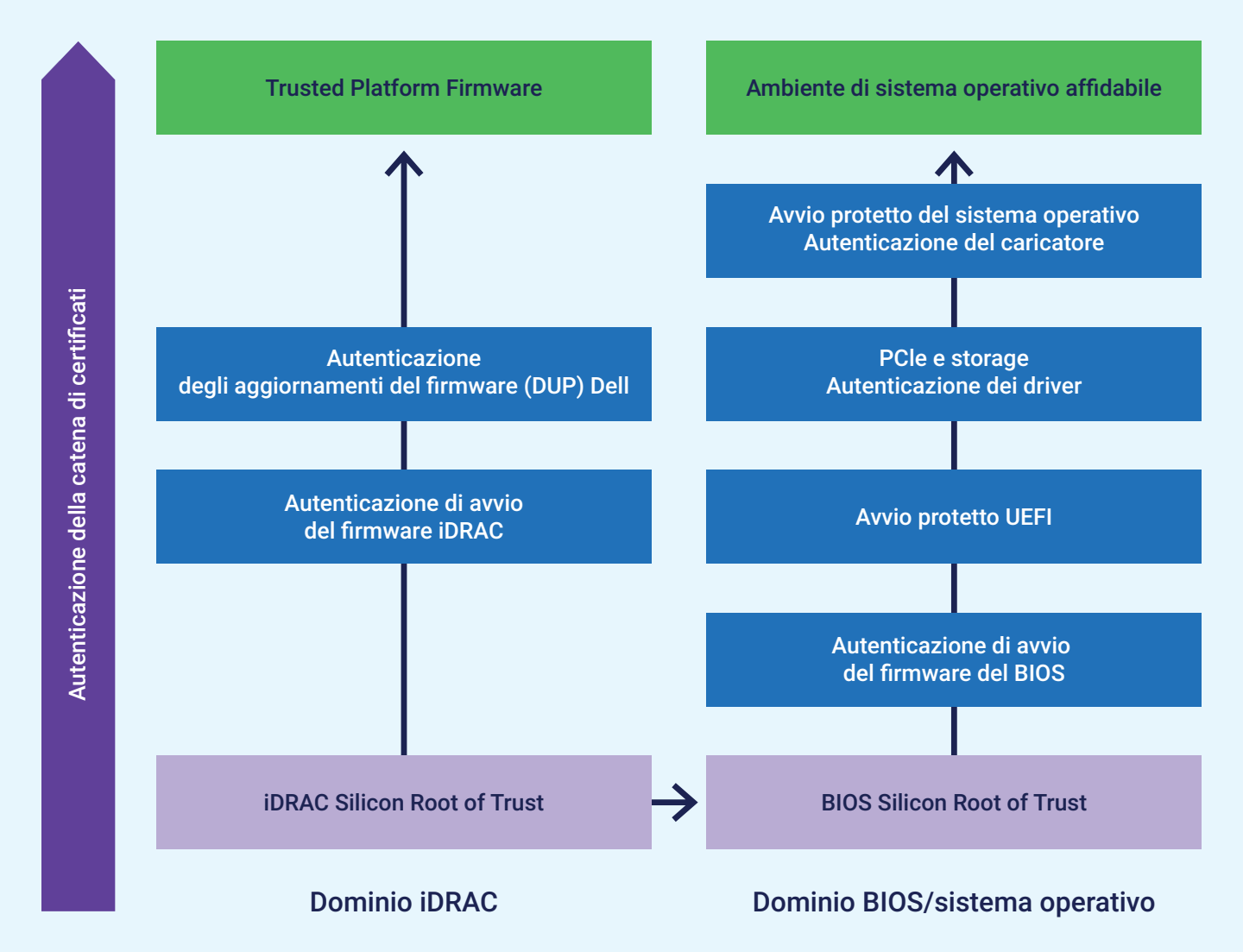

Figura 1. Domini Silicon Root of Trust nei server PowerEdge con iDRAC9.

Se la convalida del BIOS non riesce, iDRAC arresta immediatamente il server e avvisa l'utente, impedendo l'avvio di firmware non autorizzato. iDRAC include anche un sistema di backup e ripristino per il BIOS e il firmware iDRAC, che rafforza l'affidabilità del server e protegge le operazioni del server da potenziali danneggiamenti del firmware. Per fornire ulteriore protezione, iDRAC offre anche una scansione del BIOS in tempo reale che gli utenti possono eseguire su richiesta o pianificare per l'esecuzione regolare. Questa scansione richiede la licenza di iDRAC Datacenter e consente agli utenti di rilevare potenziali problemi prima del riavvio, consentendo una mitigazione proattiva.[3]

UEFI Secure Boot

I server Dell PowerEdge utilizzano lo standard di settore UEFI Secure Boot per convalidare bootloader specifici del sistema operativo, garantendo l'integrità del kernel del sistema operativo e di altri componenti critici. UEFI funge da protezione da malware e ransomware negli ambienti di preavvio. Per garantire l'interoperabilità, i produttori di server e componenti devono collaborare per garantire che il BIOS abilitato per UEFI riconosca le firme del driver e del firmware per i componenti. Convalidando le firme crittografiche dei driver UEFI e di altro codice pre-OS, UEFI Secure Boot opera per garantire che qualsiasi codice caricato durante l'avvio sia privo di contenuti dannosi.

Per migliorare la personalizzazione della sicurezza, gli amministratori possono configurare certificati di firma del bootloader del sistema operativo personalizzati per UEFI Secure Boot. (Per ulteriori informazioni sulle opzioni di UEFI Secure Boot Customization, visitare https://infohub.delltechnologies.com/section-assets/direct-from-development-uefi-boot-enhanced-security-to-combat-threats). Ciò limita l'esecuzione a bootloader del sistema operativo sicuri e affidabili, che sostengono la catena di avvio sicura autenticando il kernel e il file system del sistema operativo. Questa funzionalità offre maggiore flessibilità, in particolare per gli amministratori Linux che preferiscono firmare i propri bootloader del sistema operativo piuttosto che dipendere da CA UEFI predefinite di terze parti. Gli amministratori possono caricare i certificati personalizzati tramite l'API iDRAC, migliorando l'autenticazione dei bootloader specifici del sistema operativo. In modo esclusivo, i server Dell PowerEdge supportano la personalizzazione completa di Secure Boot, inclusa l'opzione di rimozione di tutti i certificati standard da Microsoft, VMware o UEFI CA[4]

Convalida CPLD

Ogni server Dell PowerEdge convalida il CPLD (Complex Programmable Logic Device) a ogni avvio CA. CPLD, un versatile dispositivo logico programmabile[5], comprende più PLD semplici collegati da una matrice di commutazione programmabile. Il suo firmware, generalmente memorizzato in EEPROM, memoria flash o SRAM, consente di modificare le funzioni della scheda di sistema oltre le capacità del BIOS, inclusa l'implementazione di logica specifica per le interazioni tra i dispositivi della scheda di sistema. La convalida CPLD garantisce che le modifiche alla scheda di sistema non danneggeranno i server o i dati.

Sicurezza hardware dell'iDRAC

Estendendo la catena di affidabilità ai componenti hardware aggiuntivi, iDRAC utilizza Security Protocol and Data Model (SPDM), che standardizza il modo in cui i server raccolgono le informazioni sui loro componenti. Le informazioni relative a identità, firmware e configurazione di ciascun componente sono crittografate. La sicurezza hardware di iDRAC utilizza scambi di chiavi autenticati per proteggere le linee di comunicazione tra i componenti e iDRAC. Con SPDM, iDRAC è in grado di autenticare la validità di componenti come i controller RAID PowerEdge (PERC)12 e le schede di interfaccia di rete (NIC), il che non solo migliora la sicurezza del server autenticando i certificati di identità del dispositivo dei componenti, ma avvisa anche gli utenti di eventuali errori di autenticazione.

[3] Dell, "Improved security with iDRAC9 using Root of Trust and BIOS Live Scanning", consultato il 19 dicembre 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", consultato il 4 dicembre 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", consultato il 4 dicembre 2023, https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld.

AMD Platform Secure Boot

I processori AMD sono dotati di AMD Platform Secure Boot (PSB) per contrastare un'altra crescente preoccupazione nel panorama digitale odierno: le minacce a livello di firmware. PSB sfrutta la Silicon Root of Trust RoT di AMD e verifica il processo di avvio dal codice del BIOS al bootloader del sistema operativo tramite UEFI Secure Boot.[6] Dell utilizza schede madri abilitate per AMD PSB per consentire l'esecuzione solo del codice BIOS con firma crittografica. Inoltre, Dell associa ogni processore AMD a una scheda madre specifica con fusibili programmabili una tantum che vincolano il processore alle chiavi di firma del codice del firmware Dell.[7] Per proteggersi dagli attacchi finalizzati a incorporare malware nel firmware, gli avvii PSB autorizzano solo il firmware autenticato da AMD Secure Processor.[8]

Verificando crittograficamente lo stack software, AMD Platform Secure Boot aggiunge un livello sostanziale di difesa contro le intrusioni non autorizzate sulle diverse piattaforme, in particolare in ambienti virtualizzati o nel cloud.

AMD Platform Secure Processor

Insieme a PSB, AMD Platform Secure Processor (PSP) rafforza il processo di avvio del server Dell PowerEdge. Quando una CPU si accende per la prima volta nella fabbrica Dell, AMD Platform Secure Processor incorpora un ID Dell univoco in modo permanente nella CPU. Questo ID collega in modo efficace la CPU al server PowerEdge, creando un vincolo sicuro.[9]

Questa integrazione significa che PSP impedirà l'avvio di un server PowerEdge se rileva la CPU di un altro server. Tuttavia, la portabilità della CPU è ancora possibile in caso di guasto dell'hardware. Il processore AMD è bloccato sulla chiave di firma del fornitore anziché sulla scheda madre, offrendo l'equilibrio tra sicurezza e mobilità dei componenti.[10]

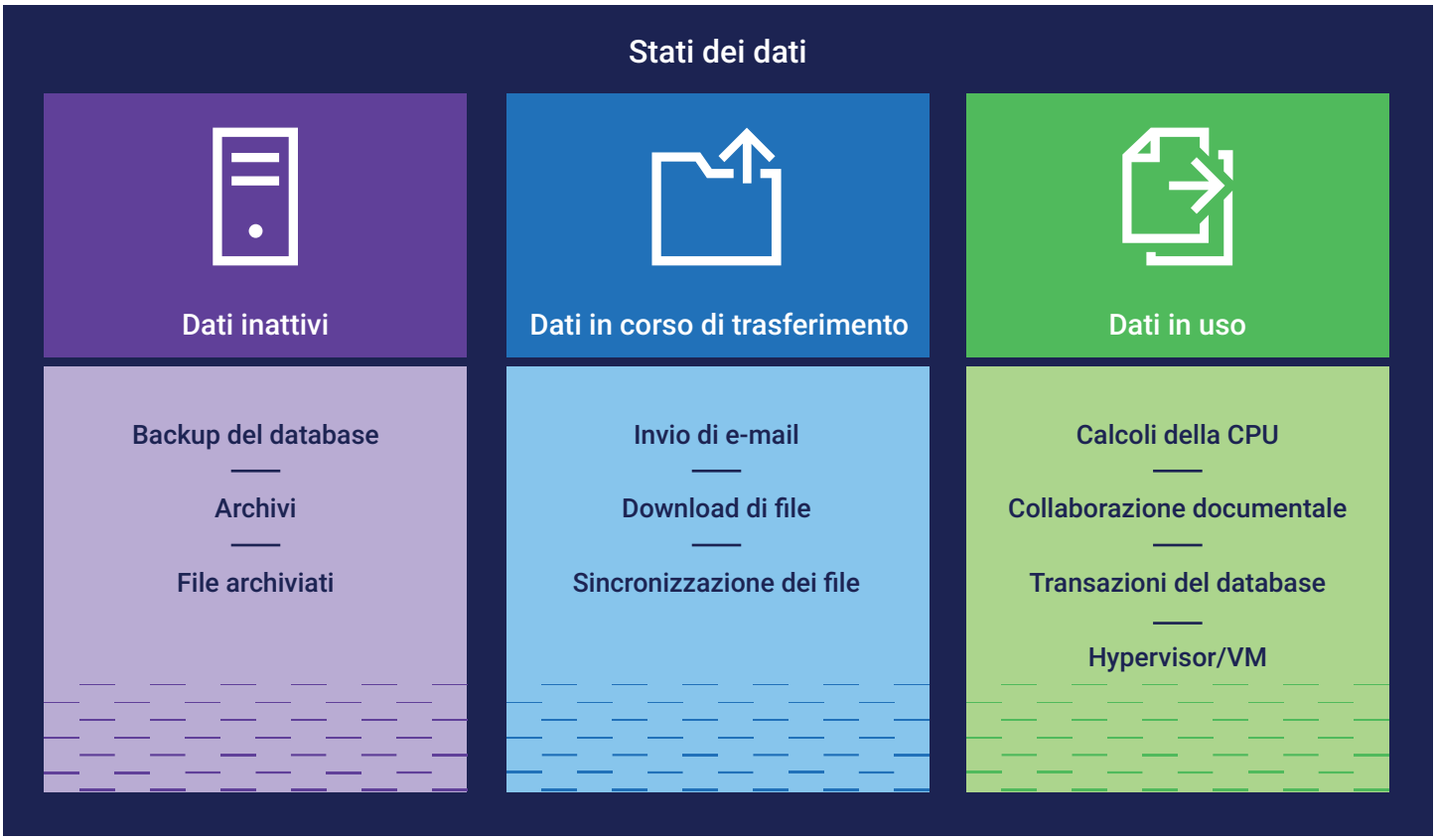

Figura 2. Stati dei dati

[6] AMD, "AMD Pro Security", consultato il 4 dicembre 2023 https://www.amd.com/en/technologies/pro-security.
[7] AMD, "AMD Infinity Guard", consultato il 4 dicembre 2023, https://www.amd.com/en/technologies/infinity-guard.
[8] AMD, "4 Ways AMD Infinity Guard Helps Protect Your Data", consultato il 4 dicembre 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", consultato il 4 dicembre 2023 https://infohub.delltechnologies.com/p/defense-in-depth-comprehensive-security-on-poweredge-amd-epyc-generation-2-rome-servers/.

Protezione dei dati

Quando gli aggressori riescono ad accedere ai sistemi, l'obiettivo finale è sempre lo stesso: trovare i tuoi dati e rubarli, manipolarli, venderli o distruggerli. Il server fisico non è l'unico punto di vulnerabilità. I malintenzionati possono attaccare la rete, le policy IT possono contenere errori, gli utenti finali possono avere password deboli e i team IT possono impostare le autorizzazioni di accesso in modo troppo poco severo. Gli utenti malintenzionati possono inviare e-mail di phishing per la distribuzione di malware.

Dell consente ai clienti di adottare un approccio Zero Trust basato su più livelli di sicurezza per proteggersi da tutti questi tipi di vulnerabilità. Per proteggersi da furti o compromissioni, devi proteggere i dati inattivi, i dati in elaborazione e i data in-flight, fino alla dismissione dei dati.[11] Con funzionalità come la crittografia at-rest, l'efficace gestione delle chiavi di crittografia e il rinnovo automatico dei certificati, i server Dell PowerEdge bloccano, scoraggiano e mitigano gli attacchi malevoli dopo il primo avvio. I server Dell PowerEdge con processori AMD offrono funzionalità aggiuntive per rafforzare la sicurezza, tra cui AMD Secure Memory Encryption (SME) e Secure Encrypted Virtualization (SEV).

Dati inattivi

Per proteggere i dati inattivi, Dell offre tre funzionalità di sicurezza principali: crittografia basata su software, gestione delle chiavi aziendali e crittografia delle unità hardware. Con le unità che supportano Instant Secure Erase (ISE), i clienti Dell possono cancellare crittograficamente tutti i dati su self-encrypted drive (SED), unità ISE e dispositivi NVM come NVDIMM. I SED proteggono i dati dagli attacchi nei casi in cui un dipendente scontento o un altro malintenzionato rimuova fisicamente le unità da un server. Poiché la password della chiave di blocco dell'unità crittografata la vincola al server specifico e al controller RAID da cui proviene, un altro server non può accedere ai dati. Per maggiore protezione, iDRAC può utilizzare Dell OpenManage Secure Enterprise Key Manager con attività di gestione delle chiavi locali (iLKM, LKM), che funziona insieme a un gestore di chiavi esterno di terze parti per bloccare e sbloccare il controller di storage all'avvio. Se qualcuno avvia il server non dal key manager, iDRAC mantiene bloccato il controller di storage in modo che i dati memorizzati sul dispositivo rimangano crittografati. Per ulteriori informazioni sulle altre opzioni delle chiavi di crittografia, visitare https://infohub.delltechnologies.com/section-assets/openmanage-sekm-storage-performance-infographic.

Data in-flight

Con i data in-flight, le vulnerabilità nella rete e il controllo degli accessi ai dati potrebbero consentire agli aggressori di intercettare o modificare i dati che viaggiano sulla rete. La connessione web iDRAC è un possibile punto di vulnerabilità, pertanto Dell fornisce diverse opzioni di protezione della connessione con un certificato TLS/SSL, riducendo così la possibilità di attacco. Sebbene questo certificato sia autofirmato per impostazione predefinita, gli amministratori possono creare un certificato personalizzato o uno firmato da una CA attendibile. Questo certificato consente connessioni crittografate e sicure per i web browser e strumenti come le utilità della riga di comando per interagire in modo sicuro con il server tramite la connessione iDRAC.

iDRAC fornisce inoltre diversi controlli che permettono agli utenti di modificare regole di accesso rigorose e limitate per l'accesso SSH al server. Per gli utenti iDRAC con la licenza di livello Datacenter, iDRAC offre il protocollo SCEP (Simple Certificate Enrollment Protocol), che conserva i certificati del web server con rinnovo automatico per evitare interruzioni accidentali della copertura. Uno studio del 2020 condotto da Principled Technologies ha rilevato che questa funzione di rinnovo automatico mantiene i server più sicuri, consentendo al personale IT di risparmiare tempo prezioso, soprattutto quando si tratta di gestire una flotta di certificati server.[12]

Dati in uso

Per proteggere i dati in uso, i server Dell PowerEdge abilitano le funzionalità di elaborazione riservate di AMD, tra cui AMD Secure Memory Encryption (SME) e Secure Encrypted Virtualization (SEV) per proteggere i dati durante il loro flusso attraverso la memoria e i componenti di elaborazione.

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

[12] Principled Technologies, “Reduce hands-on deployment times to near zero with iDRAC9 automation,” consultato il 4 dicembre 2023, https://www.principledtechnologies.com/Dell/iDRAC9-v6.10-provisioning-infographic-0323.pdf.

Secure Memory Encryption

AMD SME crittografa tutti i dati nel momento in cui entra nella memoria, proteggendo ulteriormente i dati. Senza crittografia della memoria, i dati sono vulnerabili a software dannosi e altre intrusioni, in particolare con la tecnologia di memoria più recente, come quella delle NVDIMM, che non perdono dati quando vengono spenti. Questa protezione si estende alla memoria tramite engine di crittografia a prestazioni elevate integrati nei canali di memoria, garantendo sicurezza e velocità. Poiché è completamente trasparente per il sistema operativo host e i livelli delle applicazioni, AMD SME raggiunge questo obiettivo senza richiedere modifiche al software applicativo, fornendo un approccio intuitivo per una maggiore sicurezza della memoria.[13]

La crittografia dei dati in-memory di AMD SME segna un allontanamento dai metodi di crittografia della memoria precedenti che erano personalizzati per casi d'uso specifici. Un vantaggio chiave di AMD SME è la sua flessibilità, che consente al software di utilizzarlo in diversi modi: crittografando tutta la DRAM per una protezione completa o crittografando selettivamente regioni specifiche, come quelle utilizzate dalle macchine virtuali guest (VM).[14]

AMD Secure Encrypted Virtualization

AMD SEV migliora la crittografia per la memoria e le macchine virtuali implementando un ambiente TEE (Trusted Execution Environment) basato su macchine virtuali. Integrandosi con l'architettura AMD-V, AMD SEV crittografa la memoria di ogni VM separatamente, proteggendole l'una dall'altra e dall'hypervisor. Questo approccio utilizza la crittografia per proteggere il codice all'interno di una VM da codice con privilegi più elevati potenzialmente vulnerabile, ad esempio l'hypervisor. L'ulteriore livello di sicurezza è particolarmente importante negli ambienti cloud. Questo metodo garantisce una protezione avanzata per le VM, rafforzandole contro le vulnerabilità esterne. La crittografia avviene direttamente sul controller di memoria, dove questo crittografa e decrittografa i dati senza rallentare la velocità di elaborazione, grazie ad AMD Secure Processor che gestisce tutti i dettagli della crittografia in modo invisibile.[15]

Esistono ancora alcune situazioni in cui i dati di una VM devono comunicare con altre VM o con l'hypervisor. In questi casi, AMD SEV consente alla VM di scegliere quale chiave di crittografia applicare a pagine di memoria specifiche: una chiave guest che mantiene la pagina privata per la VM o una chiave hypervisor che consente all'hypervisor e ad altre VM di decrittografare la pagina. Questa flessibilità garantisce sicurezza e comunicazione in base alle esigenze di ciascuna VM.[16]

AMD SEV offre funzionalità aggiuntive che espandono l'isolamento crittografico delle VM: SEV-Encrypted State (SEV-ES) e SEV-Secure Nested Paging (SEV-SNP). SEV-ES isola ulteriormente le VM l'una dall'altra e dall'hypervisor crittografando il contenuto del registro della CPU quando una VM si spegne, proteggendola dall'accesso non autorizzato tramite una VM vicina o l'hypervisor. SEV-SNP si basa su SEV e SEV-ES, aggiungendo protezione dell'integrità della memoria e funzionalità di protezione aggiuntive opzionali per le VM. Il miglioramento dell'integrità della memoria consente a una macchina virtuale di accedere ai dati in memoria solo se è in grado di leggere l'ultimo valore scritto. Se un'altra entità ha modificato i dati in memoria, la VM non può accedere ai dati. Ciò protegge la VM dall'esecuzione di dati o codice compromessi.

Crittografia e chiavi di crittografia

AMD SEV utilizza una chiave di crittografia univoca per ogni VM, isolando crittograficamente le VM e l'hypervisor. Questo engine di crittografia protegge i dati in scrittura e li decrittografa in lettura. Ogni VM, al momento della creazione, riceve una chiave univoca che garantisce che qualsiasi tentativo non autorizzato di accedere alla sua memoria si traduca in dati incomprensibili. Ogni processore AMD EPYC™ di quarta generazione offre fino a mille chiavi di crittografia. Questa architettura non altera le applicazioni all'interno della VM. Al contrario, opera a livello di sistema operativo e aumenta la sicurezza dei dati. Progettato per proteggere i dati in uso, incluso il contenuto della memoria, l'hardware di crittografia integrato nel controller di memoria gestisce la crittografia e la decrittografia del traffico VRAM, rafforzando la protezione dei dati in uso.[17]

[13] AMD, "AMD Infinity Guard."
[14] AMD, "AMD Memory Encryption", consultato il 4 dicembre 2023, https://www.amd.com/content/dam/amd/en/documenti/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf.
[15] AMD, "AMD Secure Encrypted Virtualization", consultato il 4 dicembre 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".

Conclusione

Dal momento in cui ordini i server Dell PowerEdge con processori AMD fino al ritiro e in ogni momento intermedio, Dell e AMD offrono numerosi livelli di sicurezza per mantenere i tuoi dati al sicuro. Grazie a livelli strettamente integrati di Silicon Root of Trust e più livelli di protezione all'avvio per eliminare driver, firmware e versioni del BIOS sospetti, i componenti del server sono protetti fin dal momento della produzione. Inoltre, grazie alla crittografia delle unità SED e ISE, i dati sono al sicuro anche se malintenzionati rimuovono fisicamente dischi o server dal data center. Grazie ad altre funzionalità di protezione, come la tecnologia AMD SME e SEV basata su processori, che proteggono i dati in elaborazione, e ai i controlli software all'avanguardia tramite iDRAC, i server Dell PowerEdge con processori AMD contribuiscono a garantire che l'attività prosegua senza intoppi, indipendentemente dai nuovi metodi di attacco che i criminali informatici possono escogitare. Per ulteriori informazioni sui server Dell PowerEdge con processori AMD EPYC di 4a generazione, visita www.dell.com/servers/amd.

Ulteriori informazioni sulle soluzioni Dell e AMD

Contatta un esperto Dell Technologies

Visualizza altre risorse

Partecipa alla conversazione con #PowerEdge

DELL Technologies

AMD together we advance_

Pubblicato negli Stati Uniti, 1/24 White paper