DELL Technologies

Microsoft

White paper

Protezione avanzata con le funzionalità combinate di Windows Server 2022 e i server Dell EMC™ PowerEdge™ di nuova generazione

Rinforzare i carichi di lavoro business-critical con un ambiente più sicuro per l'hardware, il firmware e il sistema operativo

Secondo Cybersecurity Ventures, il crimine informatico globale costerà 6 trilioni di dollari nel 2021 e raggiungerà 10,5 trilioni di dollari nel 2025[1]. I soli attacchi ransomware sono aumentati di 61 volte in sei anni, toccando i 20 miliardi di dollari nel 2021, con una frequenza di un attacco ogni 11 secondi[1]. Una survey di IDC del 2021 ha rilevato che più di un terzo delle organizzazioni intervistate in tutto il mondo ha subito almeno un attacco ransomware o una violazione negli ultimi 12 mesi[2]. Sebbene IBM abbia stimato che il costo attuale di una singola violazione dei dati sia pari a 4,24 milioni di dollari[3], il costo reale delle violazioni può essere molto più elevato. Ci sono stati casi di ospedali negli Stati Uniti che hanno dovuto dirottare i pazienti del Pronto soccorso in altri ospedali e respingere le ambulanze a causa degli attacchi ransomware[4].

Gli attacchi al firmware possono essere una minaccia particolarmente insidiosa per le organizzazioni, perché possono impiantare malware prima che sia avviato il sistema operativo e le relative misure di sicurezza basate sul software in esecuzione su tale sistema. Eppure, meno della metà delle organizzazioni ha intrapreso iniziative per rafforzare i sistemi contro gli attacchi al firmware, nonostante la loro frequenza sia quintuplicata negli ultimi cinque anni.[5] Alla fine, i carichi di lavoro sono sicuri solo nella misura in cui è protetto l'intero stack su cui vengono eseguiti.

Per affrontare questa crescita esponenziale in termini di frequenza, varietà e costi delle minacce malware, la sicurezza moderna deve essere multilayer. I malware, infatti, possono compromettere i sistemi a livello di hardware e firmware o durante l'avvio, ovvero in tutte le aree in cui la sicurezza software-defined è impotente. Per contrastare questa vulnerabilità, la strategia per la sicurezza moderna dei server non può essere monolitica, ma deve essere integrata nell'intero stack dell'infrastruttura. La combinazione dei server Dell EMC™ PowerEdge™ di nuova generazione e Windows Server 2022 semplifica l'importante compito degli amministratori di allineare hardware, firmware e sistema operativo al fine di proteggere adeguatamente i carichi di lavoro business-critical.

I vantaggi della combinazione dei server con core protetto di Windows Server 2022 e dei server PowerEdge di nuova generazione

Il server con core protetto è una novità di Windows Server 2022 che utilizza funzionalità hardware, firmware e del sistema operativo per proteggere i sistemi dalle minacce attuali e future. La combinazione del software dei server con core protetto di Windows Server 2022 eseguito sull'hardware dei server PowerEdge di nuova generazione offre tre importanti vantaggi alle organizzazioni:

- Protezione avanzata
- Difesa preventiva
- Sicurezza semplificata

Protezione avanzata

In base ai dati di Threat Intelligence di Microsoft, i PC con core protetto offrono una protezione più che doppia contro le infezioni rispetto ai normali PC. Microsoft ora sta introducendo questa tecnologia nei server con core protetto di Windows Server 2022.[5] Le misure di protezione abilitate da un server con core protetto consentono di creare una piattaforma sicura per i carichi di lavoro e i dati critici sul server. Nello specifico, i server con core protetto utilizzano il supporto del processore per la tecnologia Dynamic Root of Trust for Measurement (DRTM) per inserire il firmware in una sandbox basata su hardware. Questo isolamento consente di limitare l'impatto delle vulnerabilità in milioni di righe di codice firmware con privilegi elevati.

Integrando l'isolamento del firmware in Windows Server 2022, la sicurezza basata sulla virtualizzazione (VBS, Virtualization-Based Security) isola le parti critiche del sistema operativo, ad esempio il kernel, dal resto del sistema. In questo modo, i server restano dedicati all'esecuzione dei carichi di lavoro critici e le applicazioni e i dati correlati sono protetti dagli attacchi e dal rischio di fuoriuscita.

Per rafforzare ulteriormente il firmware nei server PowerEdge contro gli attacchi, Dell Technologies ha aumenta la protezione della supply chain per i server PowerEdge per garantire che nessuno possa manomettere il server durante il trasporto dalla fabbrica al sito del cliente (ulteriori dettagli sono illustrati più dettagliatamente nella sezione seguente Sicurezza aggiuntiva con l'integrità della supply chain di Dell Technologies).

Difesa preventiva

Le funzionalità con core protetto aiutano a difendersi e a bloccare in modo proattivo molti percorsi che i malintenzionati potrebbero utilizzare per sfruttare i sistemi. L'integrità del codice con protezione dell'hypervisor (HVCI, Hypervisor-protected Code Integrity) in VBS isola la funzione decisionale per l'integrità del codice (CI, Code Integrity) dal resto del sistema operativo Windows. Così facendo, l'unico modo per rendere eseguibile la memoria kernel è tramite una verifica CI. VBS consente inoltre di utilizzare Windows Defender Credential Guard, che archivia i segreti e le credenziali utente in un container virtuale al quale il sistema operativo non può accedere direttamente.

Trusted Platform Module 2.0 (TPM 2.0) è un componente standard dei server con core protetto e fornisce un archivio protetto per le chiavi e i dati sensibili, come le misurazioni dei componenti caricati durante l'avvio. La possibilità di verificare che il firmware eseguito durante l'avvio abbia una firma valida dell'autore previsto e non sia stato manomesso contribuisce a migliorare la sicurezza. Questa Root of Trust hardware migliora anche la protezione fornita da funzionalità come BitLocker Drive Encryption, che utilizza TPM 2.0 e facilita la creazione di flussi di lavoro basati su attestazione che possono essere incorporati nelle strategie di sicurezza Zero Trust. Nel complesso, queste difese consentono ai team IT e SecOps di utilizzare meglio il proprio tempo, dedicandosi alle molte aree della sicurezza che richiedono la loro attenzione.

I server PowerEdge di nuova generazione supportano lo standard di settore Avvio sicuro UEFI (Unified Extensible Firmware Interface). Avvio sicuro UEFI controlla le firme crittografiche dei driver UEFI e dell'altro codice caricato prima dell'esecuzione del sistema operativo per verificare che il malware non abbia manomesso il firmware. Inoltre, i server PowerEdge supportano TPM 2.0 per migliorare la sicurezza del firmware e del sistema operativo.

Sicurezza semplificata

Con l'acquisto di un server PowerEdge con core protetto, si ha la certezza di avere a disposizione un set di hardware, firmware e driver di Dell Technologies in grado di garantire la massima sicurezza. Microsoft collabora strettamente con Dell Technologies per semplificare l'abilitazione delle misure di sicurezza sui server PowerEdge.

Le nuove funzionalità di Windows Admin Center consentono agli amministratori di configurare facilmente le funzionalità di protezione del sistema operativo dei server con core protetto di Windows Server 2022. La nuova funzionalità di sicurezza di Windows Admin Center consente agli amministratori di abilitare la sicurezza avanzata con un semplice clic. Windows Admin Center mostra lo stato di tutte le funzionalità di protezione necessarie per i server con core protetto di Windows Server 2022 e consente agli amministratori di attivare le funzionalità in base alle necessità da un'unica posizione.

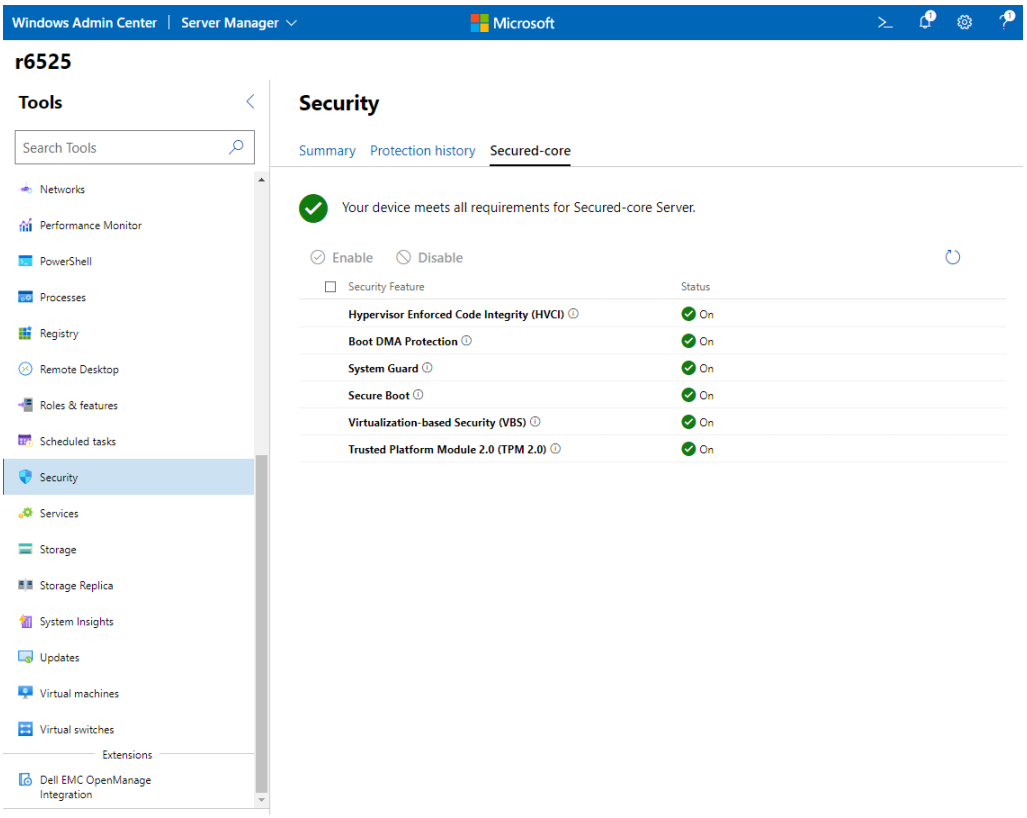


Figura 1. Schermata di conferma dei server con core protetto in Windows Admin Center

Dell EMC™ OpenManage™ Integration with Windows Admin Center è un'estensione per Windows Admin Center che semplifica ulteriormente la gestione dei server con core protetto. Tra le altre cose, questa estensione semplifica le attività di sicurezza degli amministratori IT gestendo in remoto i server PowerEdge. Nel contesto dei server con core protetto di Windows Server 2022, l'estensione OpenManage Integration with Windows Admin Center consente di visualizzare l'inventario dei server PowerEdge da Windows Admin Center e fornisce una vista unificata delle informazioni su stato, hardware e firmware dell'inventario per i componenti dei server PowerEdge.

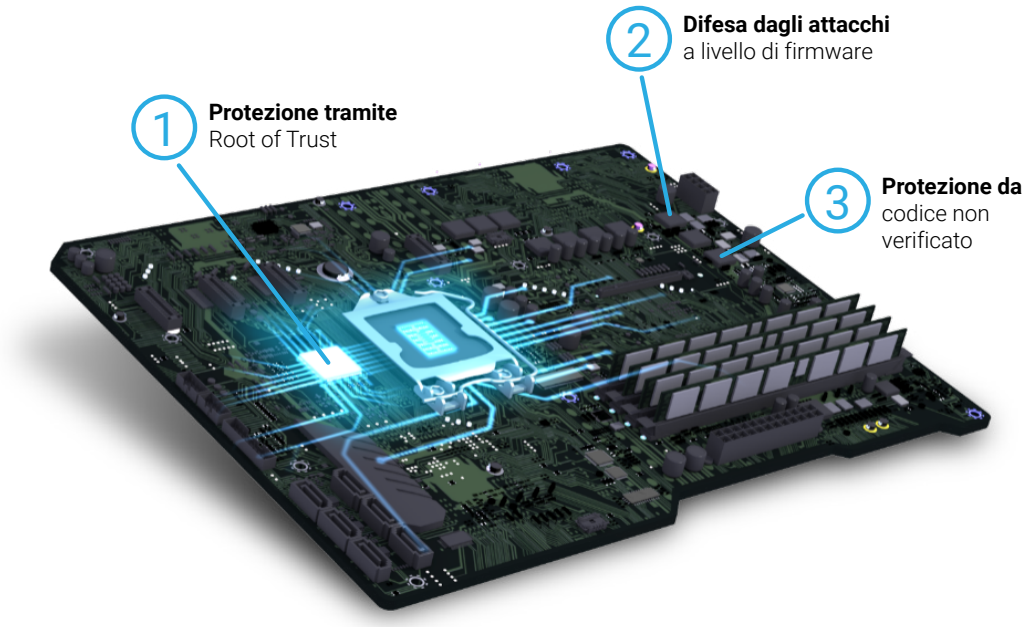
Supporto dei server PowerEdge per i server con core protetto di Windows Server 2022

A causa della natura multilayer delle difese dei server con core protetto, è fondamentale poter contare sul supporto dell'OEM dell'hardware. I server PowerEdge sono testati e certificati da Dell Technologies per garantire che l'hardware e il firmware soddisfino i requisiti delle funzionalità di protezione di Windows Server 2022. Inoltre, l'hardware e il firmware nei server PowerEdge sono configurati per abilitare il server con core protetto di Windows Server 2022. La Tabella 1 descrive in dettaglio in che modo l'hardware dei server PowerEdge supporta le funzionalità di Windows Server 2022.

Tabella 1. Mappatura delle funzionalità di protezione di Windows Server 2022 e delle principali funzionalità di supporto nei server Dell EMC™ PowerEdge™ di nuova generazione

	Windows Server 2022	Server Dell EMC™ PowerEdge™ di nuova generazione
Protezione avanzata	I sistemi con core protetto inseriscono il firmware in una sandbox basata su hardware, contribuendo a limitare l'impatto delle vulnerabilità basate su firmware. VBS isola le parti critiche del sistema operativo, proteggendole dal malware avanzato.	Dell Technologies aiuta a proteggere la supply chain per i server PowerEdge per garantire che nessuno possa manomettere il server o compromettere il firmware durante il trasporto dalla fabbrica al sito del cliente.
Difesa preventiva	Le funzionalità VBS come HVCI e Windows Defender Credential Guard bloccano intere classi di vulnerabilità e proteggono meglio gli asset sensibili come le credenziali. TPM 2.0 fornisce una Root of Trust hardware, che viene utilizzata come base per la sicurezza.	I server PowerEdge supportano lo standard di settore Avvio sicuro UEFI per controllare le firme crittografiche dei driver UEFI e dell'altro codice caricato prima dell'esecuzione del sistema operativo. I server PowerEdge supportano TPM 2.0.
Sicurezza semplificata	Windows Admin Center fornisce un facile accesso per configurare i server con core protetto.	Microsoft collabora con Dell Technologies per semplificare l'abilitazione delle misure di sicurezza sui server PowerEdge. L'estensione Dell EMC™ OpenManage™ Integration with Windows Admin Center semplifica ulteriormente la gestione dei server con core protetto.

Anatomia della sicurezza avanzata multilayer



1 Protezione tramite Root of Trust

Grazie alla partnership con i principali OEM, come Dell Technologies, e con fornitori di processori come Intel e AMD, i server con core protetto utilizzano lo standard di settore Root of Trust hardware, abbinato a funzionalità di sicurezza integrate nelle moderne CPU.

I server con core protetto utilizzano TPM 2.0 e una CPU moderna con DRTM per avviare i server in modo più sicuro e ridurre al minimo le vulnerabilità del firmware.

2 Difesa contro gli attacchi a livello di firmware

I server con core protetto utilizzano la sicurezza basata su hardware della CPU moderna per avviare il sistema in uno stato affidabile, impedendo ai malware avanzati di manomettere il sistema e bloccando gli attacchi a livello del firmware.

System Guard Secure Launch utilizza la CPU per convalidare il dispositivo e garantire un avvio più sicuro, contribuendo a prevenire attacchi avanzati al firmware.

3 Protezione contro il codice non verificato

Il codice in esecuzione all'interno della base di elaborazione affidabile viene eseguito con funzionalità di integrità e non è soggetto a exploit o attacchi.

Abilitato con HVCI, un server con core protetto avvia solo gli eseguibili firmati da autorità note e approvate. L'hypervisor imposta e applica le autorizzazioni per impedire che il malware tenti di modificare la memoria e di renderla eseguibile.

Supporto di server PowerEdge di nuova generazione per la connettività sicura in Windows Server 2022

I server PowerEdge di nuova generazione supportano la crittografia AES-256 Server Message Block (SMB) per i carichi di lavoro che richiedono livelli maggiori di sicurezza. Ciò significa che i server PowerEdge che eseguono Windows Server 2022 sono in grado di fornire una crittografia end-to-end ai dati dei carichi di lavoro per aumentare la sicurezza. La crittografia AES a 256 bit utilizzata per SMB in Windows Server 2022 è sufficientemente robusta da resistere anche agli attacchi di forza bruta sferrati da computer quantum, se le password sono abbastanza complesse.

I server PowerEdge e Windows Server 2022 estendono ulteriormente la crittografia SMB end-to-end dai singoli server alle comunicazioni interne dei cluster con la crittografia AES-256 per il traffico di dati SMB est-ovest. Questi controlli aggiuntivi di crittografia SMB difendono ulteriormente i carichi di lavoro e sbarrano eventuali accessi agli attacchi.

Infine, Windows Server 2022 utilizza Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), incluso nei processori scalabili Intel® Xeon® di terza generazione, e la crittografia vettoriale AES a 256 bit (vAES256), inclusa nei processori AMD EPYC™ Zen 3. Questi set di istruzioni per processori avanzati migliorano le prestazioni della crittografia AES-256 nei server PowerEdge. Sfruttando queste tecnologie di sicurezza avanzate, Dell Technologies e Microsoft sollevano gli utenti dall'onere di scegliere tra una sicurezza affidabile e la reattività per i carichi di lavoro business-critical.

Sicurezza aggiuntiva con l'integrità della supply chain di Dell Technologies

L'integrità della supply chain di Dell Technologies impedisce la manomissione dei componenti hardware e firmware durante la produzione e la spedizione. Nell'ambito dell'integrità dell'hardware, Dell Technologies si impegna a garantire che non vi sia alcuna manomissione o inserimento di componenti contraffatti prima della spedizione dei prodotti ai clienti. I controlli messi in atto da Dell Technologies riguardano la selezione dei fornitori, l'approvvigionamento, i processi di produzione e la governance attraverso procedure di verifica e test. Le ispezioni dei materiali durante la produzione permettono di identificare i componenti che sono contrassegnati in modo errato, si discostano dai normali parametri delle prestazioni o contengono un ID elettronico non corretto.

Per garantire l'integrità del software, Dell Technologies controlla che non venga inserito alcun malware nei driver del firmware o del dispositivo prima della spedizione di un prodotto al cliente e inoltre cerca di prevenire eventuali vulnerabilità di codifica. Dell Technologies mantiene la certificazione ISO 9001 per tutti i siti di produzione globali. Il rispetto rigoroso di questi processi e controlli riduce al minimo il rischio che componenti contraffatti vengano incorporati nei prodotti Dell Technologies™ o che nel firmware o nei driver dei dispositivi vengano inseriti malware. Inoltre, Dell Technologies implementa queste misure nell'ambito del processo SDLC (Software Development Lifecycle).

Dell Technologies si impegna anche a garantire la sicurezza fisica delle strutture di produzione e delle catene di trasporto. Dell Technologies ha bisogno di determinati stabilimenti in cui i suoi prodotti vengano realizzati in conformità con i requisiti di sicurezza degli impianti TAPA (Transported Asset Protection Association), tra cui l'utilizzo di telecamere a circuito chiuso monitorate in aree chiave, il controllo degli accessi e la costante sorveglianza di ingressi e uscite. Dell Technologies ha anche messo in atto misure di difesa per proteggere i prodotti da furti e manomissioni durante il trasporto, nell'ambito di un programma logistico leader del settore. Infine, la verifica SCV (Secured Component Verification) di Dell Technologies per i server PowerEdge consente ai clienti Dell Technologies di verificare che il server PowerEdge ricevuto dal cliente corrisponda a quello prodotto in fabbrica.

Protezione dei carichi di lavoro essenziali con una base per la sicurezza più solida grazie a Windows Server 2022 e ai server Dell EMC PowerEdge di nuova generazione

I carichi di lavoro sono sicuri solo nella misura in cui è protetta la base su cui vengono eseguiti. La minaccia proveniente da malware e violazioni dei dati è destinata a crescere, soprattutto perché i malintenzionati continueranno a esplorare canali di attacco non coperti dalle misure di sicurezza tradizionali basate su software. Gli attacchi al firmware dei server di solito vengono sferrati durante il processo di avvio, quando la sicurezza basata su software non ha ancora iniziato a proteggere i sistemi. La protezione moderna dei server deve essere eterogenea e distribuita su più livelli che comprendano hardware, firmware e sistema operativo.

L'aggiornamento a Windows Server 2022 oggi ha particolarmente senso, perché la funzionalità dei server con core protetto di Windows Server 2022 aiuta le organizzazioni a contrastare le minacce sia al firmware che al sistema operativo. Insieme alle misure di protezione dell'integrità hardware e software di Dell Technologies, i server Dell EMC PowerEdge di nuova generazione che eseguono Windows Server 2022 possono fornire una sicurezza moderna all'intero stack di hardware, firmware e sistema operativo. Le funzionalità di connettività sicura di Windows Server 2022, supportate nei server PowerEdge di nuova generazione, estendono la protezione dai singoli server agli interi cluster all'interno del data center. Inoltre, visto che il supporto per Windows Server 2012 termina a ottobre 2023, è il momento giusto per iniziare a elaborare dei piani di aggiornamento.[6]

Per ulteriori informazioni su come Windows Server 2022 e i server Dell EMC PowerEdge di nuova generazione possono contribuire a proteggere i carichi di lavoro e i dati critici, visitare www.delltechnologies.com/en-us/solutions/microsoft-oem/.

[1] Cybersecurity Ventures. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025". Novembre 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
[2] IDC. "IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach". Agosto 2021.
[3] IBM. "How much does a data breach cost?". 2021. www.ibm.com/security/data-breach.
[4] Dan Goodin. "Hospitals hamstrung by ransomware are turning away patients". *Ars Technica.* Agosto 2021. https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/.
[5] Microsoft. "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats". Marzo 2021. www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/.
[6] Alla data di stesura di questo documento. Per informazioni più aggiornate sulla fine del supporto per Windows Server 2012, visitare la pagina relativa al ciclo di vita di Windows Server 2012: https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Modernizzazione con Windows Server 2022.
Il sistema operativo predisposto per il cloud che incrementa gli investimenti on-premise con funzionalità ibride.