DELL Technologies

White paper

White paper tecnico: Sicurezza cyber-resiliente nei server Dell EMC PowerEdge

Dicembre 2020

Revisioni

Data	Descrizione
Gennaio 2018	Release iniziale
Novembre 2020	Versione rivista

Sommario

Sommario

Executive Summary

L'approccio alla sicurezza di Dell Technologies è di tipo intrinseco, non viene aggiunto a posteriori ed è perfettamente integrato in ogni fase del processo Secure Development Lifecycle di Dell. Ci impegniamo a sviluppare continuamente controlli, funzioni e soluzioni di sicurezza PowerEdge per soddisfare scenari di minacce in costante evoluzione e continuiamo a stabilizzare la sicurezza mediante Silicon Root of Trust. Questo documento fornisce informazioni dettagliate sulle funzionalità di protezione integrate nella piattaforma cyber-resiliente PowerEdge, molte delle quali sono abilitate da integrated Dell Remote Access Controller (iDRAC9). Sono state aggiunte molte nuove funzioni dal precedente white paper sulla sicurezza PowerEdge, che spaziano dal controllo degli accessi alla crittografia dei dati e alla garanzia della supply chain. Questi comprendono: Live BIOS Scanning, personalizzazione di UEFI Secure Boot, autenticazione a più fattori RSA SecurID, Secure Enterprise Key Management (SEKM), Secured Component Verification (SCV), System Erase avanzato, iscrizione e rinnovo automatici dei certificati, Cipher Select e supporto CNSA. Tutte le funzioni sono caratterizzate da un utilizzo intensivo di intelligence e automazione per tenere il passo con la curva delle minacce e consentire il dimensionamento richiesto da modelli di utilizzo in continua espansione.

1. Introduzione

Con l'evolversi del panorama delle minacce, i professionisti dell'IT e della sicurezza cercano in ogni modo di gestire i rischi per i dati e le risorse. I dati vengono utilizzati in molti dispositivi, on-premise e nel cloud e continuano ad accumularsi eventi di violazione dei dati ad alto impatto. Da sempre la sicurezza viene posta con maggiore enfasi sul sistema operativo, sulle applicazioni, sui firewall e sui sistemi IPS e IDS, che continuano a rappresentare importanti aree di interesse. Tuttavia, alla luce degli eventi degli ultimi due anni che hanno evidenziato minacce all'hardware, consideriamo altrettanto fondamentale la necessità di proteggere i componenti dell'infrastruttura basata su hardware come firmware, BIOS, BMC e altre protezioni hardware, tra cui la garanzia della supply chain.

Secondo il Digital Transformation Index 2020 di Dell Technologies, la riservatezza dei dati e i dubbi in materia di sicurezza informatica rappresentano la barriera principale alla Digital Transformation.[1] Il 63% delle aziende ha affrontato situazioni di rischio in ambito di dati a causa di una vulnerabilità[2]. I danni globali associati alla criminalità informatica raggiungeranno i 6 mila miliardi di dollari nel 2021[3].

In un momento in cui i server diventano più critici in un'architettura di software-defined data center, la sicurezza dei server rappresenta ora la base per la sicurezza aziendale a 360 gradi. I server devono enfatizzare la sicurezza a livello di hardware e firmware, sfruttando una radice di affidabilità non modificabile che può essere utilizzata per verificare le operazioni successive all'interno del server. In questo modo viene stabilita una catena di certificati che si estende per l'intero ciclo di vita del server, dal deployment alla manutenzione, fino alla dismissione.

I server Dell EMC PowerEdge di 14ª e 15ª generazione con iDRAC9 forniscono una catena di certificati che, combinata con controlli di sicurezza e strumenti completi di gestione, assicura solidi livelli di sicurezza dell'hardware e del firmware. Il risultato è un'architettura cyber-resiliente che include al suo interno ogni aspetto del server, tra cui il firmware del server integrato, i dati archiviati nel sistema, il sistema operativo, le periferiche e le operazioni di gestione. Le organizzazioni possono creare un processo per proteggere la loro preziosa infrastruttura server e i dati che contiene, rilevare eventuali anomalie, operazioni non autorizzate o violazioni ed eseguire il ripristino da eventi non intenzionali o dannosi.

[1] Digital Transformation Index 2020 di Dell Technologies

[2] Match Present-Day Security threats with BIOS-Level Control. Documento di Forrester Consulting sulla leadership di pensiero commissionato da Dell, 2019

[3] Ransomware Attacks Predicted to Occur... The National Law Review, 2020

2. Il percorso verso un'infrastruttura server sicura

I server Dell EMC PowerEdge offrono da varie generazioni un livello efficace di sicurezza, che include l'impiego innovativo della sicurezza dei dati basata sul silicio. I server Dell EMC PowerEdge 14G hanno esteso la sicurezza basata sul silicio per l'autenticazione del BIOS e del firmware con una radice di affidabilità crittografica durante il processo di avvio dei server. Il team di prodotti Dell EMC ha tenuto conto di vari requisiti essenziali durante la progettazione della 14ª e 15ª generazione di server PowerEdge in risposta alle minacce alla sicurezza affrontate nei moderni ambienti IT:

- **Protezione.** Protegge il server durante ogni aspetto del ciclo di vita, includendo BIOS, firmware, dati e hardware fisico.
- **Rilevamento:** Rilevamento degli attacchi informatici e delle modifiche non approvate; coinvolgimento degli amministratori IT in modo proattivo.
- **Ripristino:** Ripristino di BIOS, firmware e OS all'ultima configurazione corretta; ritiro o riutilizzo sicuro di server.

I server Dell EMC PowerEdge sono conformi ai principali standard di settore per la crittografia e la sicurezza definiti in questo documento ed eseguono continuamente il monitoraggio e la gestione di nuove vulnerabilità.

Dell EMC ha integrato la sicurezza nel processo Security Development Lifecycle come elemento chiave in ogni aspetto dello sviluppo, dell'approvvigionamento, della produzione, della spedizione e del supporto, creando a tutti gli effetti un'architettura cyber-resiliente.

2.1 Security Development Lifecycle

Per garantire un'architettura cyber-resiliente occorrono consapevolezza della sicurezza e rigore in ciascuna fase dello sviluppo. Questo processo è il cosiddetto modello Security Development Lifecycle (SDL), in cui la sicurezza non è un aspetto da affrontare in un secondo momento, ma è parte integrante del processo generale di progettazione dei server. Questo processo di progettazione include la considerazione delle esigenze di sicurezza in tutto il ciclo di vita dei server, come illustrato nell'elenco sottostante e indicato nella Figura 1:

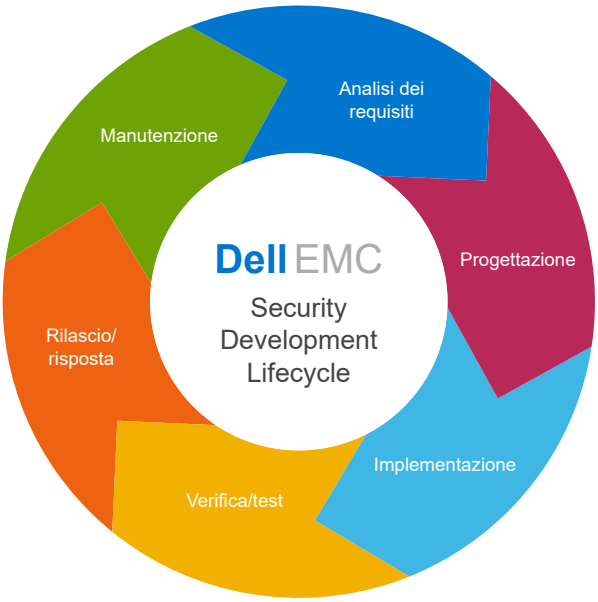


Figura 1: Security Development Lifecycle di Dell EMC

- Le funzioni sono concepite, progettate, trasformate in prototipi, implementate, messe in produzione, installate e gestite secondo un criterio prioritario che è quello della sicurezza
- Il firmware del server è progettato in modo da bloccare, ostacolare e contrastare l'introduzione di codice malevole durante tutte le fasi del ciclo di vita dello sviluppo del prodotto
  - » Copertura dei test di penetrazione e modellazione delle minacce durante il processo di progettazione
  - » Vengono applicate procedure di codifica sicure in ogni fase dello sviluppo del firmware
- Per le tecnologie critiche, alcuni audit esterni integrano il processo SDL interno per garantire che il firmware sia conforme alle best practice note in ambito di sicurezza
- Vengono eseguiti test e valutazioni costanti di nuove potenziali vulnerabilità utilizzando i più recenti strumenti di valutazione della sicurezza
- Risposta rapida a eventi CVE (Common Vulnerabilities and Exposures, vulnerabilità ed esposizioni comuni) di importanza critica, incluse misure di correzione consigliate, se garantite.

2.2 Un'architettura cyber-resiliente

I server Dell EMC PowerEdge di 14ª e 15ª generazione offrono un'architettura cyber-resiliente migliorata con un design rinforzato dei server per la protezione, il rilevamento e il ripristino dagli attacchi informatici. Ecco alcune caratteristiche principali di questa architettura:

- **Protezione efficace dagli attacchi**
  - » Silicon Root of Trust
  - » Avvio protetto
  - » Aggiornamenti firmware firmati
  - » Dynamic System Lockdown
  - » Crittografia del disco rigido ed Enterprise Key Management
- **Rilevamento affidabile degli attacchi**
  - » Rilevamento delle deviazioni a livello di configurazione e firmware
  - » Registrazione persistente degli eventi
  - » Audit log e avvisi
  - » Rilevamento delle intrusioni nello chassis
- **Ripristino rapido con interruzioni del business minime o assenti**
  - » Ripristino automatico del BIOS
  - » Ripristino rapido del sistema operativo
  - » Rollback del firmware
  - » Erasure rapida del sistema

2.3 Le minacce di oggi

Sono molti i vettori di minacce nel mutevole panorama di oggi. La Tabella 1 sintetizza l'approccio di Dell EMC alla gestione delle minacce back-end critiche.

Tabella 1: Modi in cui Dell EMC gestisce i comuni vettori di minacce

Livelli della piattaforma server		
Livello di sicurezza	**Vettore di minacce**	**Soluzione Dell EMC**
Server fisico	Manomissioni di server/componenti	Secured Component Verification (SCV), rilevamento delle intrusioni nello chassis
Firmware e software	Danneggiamento del firmware, malware injection	Silicon Root of Trust, Intel Boot Guard, AMD Secure Root of Trust, personalizzazione di UEFI Secure Boot Firmware con convalida e firma crittografica
	Software	Reporting CVE, applicazione di patch in base alle esigenze
Funzioni di attendibilità delle attestazioni	Spoofing dell'identità dei server	TPM, TXT, catena di certificati
Gestione server	Configurazione, aggiornamenti e attacchi a porte aperte non autorizzati	iDRAC9. Attestazione remota

Livelli dell'ambiente server		
Livello di sicurezza	**Vettore di minacce**	**Soluzione Dell EMC**
Dati	Violazioni dei dati	SED (Self-Encrypting Drive): FIPS oppure Opal/TCG Secure Enterprise Key Management, unità solo ISE (Instant Secure Erase) Autenticazione sicura degli utenti
Integrità della supply chain	Componenti contraffatti	Certificazione ISO9001 per tutti i siti di produzione di server globali, Secured Component Verification, prova di possesso
	Minacce malware	Misure di sicurezza implementate nell'ambito del processo SDL (Secure Development Lifecycle)
Sicurezza della supply chain	Sicurezza fisica nei siti di produzione	Requisiti di sicurezza degli impianti TAPA (Transported Asset Protection Association)
	Furto e manomissione durante il trasporto	Customs-Trade Partnership Against Terrorism (C-TPAT), SCV

3. Protezione

La funzione di protezione è una componente chiave del NIST Cybersecurity Framework e previene gli attacchi di sicurezza informatica. Questa funzione è costituita da diverse categorie, tra cui controllo degli accessi, sicurezza dei dati, manutenzione e tecnologia di protezione. La filosofia sottostante è che gli asset dell'infrastruttura devono fornire una solida protezione da accessi non autorizzati a risorse e dati nell'ambito di un ambiente informatico e di installazione sicuro e completo, inclusa la protezione da modifiche non autorizzate di componenti critici come BIOS e firmware. La piattaforma soddisfa le attuali raccomandazioni in ambito di NIST SP 800-193.

L'architettura cyber-resiliente nei server PowerEdge offre un livello elevato di protezione della piattaforma che include le seguenti funzionalità:

- Avvio protetto verificato tramite crittografia
- Sicurezza dell'accesso degli utenti
- Aggiornamenti firmware firmati
- Storage dei dati crittografato
- Protezione fisica
- Integrità e sicurezza della supply chain

3.1 Avvio protetto verificato tramite crittografia

Uno degli aspetti più critici della sicurezza dei server consiste nel garantire che il processo di avvio possa essere verificato come sicuro. Questo processo offre un punto di riferimento affidabile per tutte le operazioni successive, come l'avvio del sistema operativo o l'aggiornamento del firmware. I server PowerEdge utilizzano la sicurezza basata sul silicio da varie generazioni per funzioni come iDRAC Credential Vault, una memoria sicura crittografata in iDRAC per l'archiviazione dei dati sensibili. Il processo di avvio viene verificato mediante Silicon Root of Trust per rispettare le indicazioni NIST SP 800-147B ("Linee guida di protezione del BIOS per server") e NIST SP 800-155 ("Linee guida di misurazione dell'integrità del BIOS").

3.1.1 Silicon Root of Trust

I server PowerEdge di 14ª e 15ª generazione (basati su Intel o AMD) utilizzano ora una Silicon Root of Trust non modificabile per attestare l'integrità del BIOS e del firmware iDRAC. Questa tecnologia si basa su chiavi pubbliche one-time programmabili e read-only che garantiscono la protezione contro le manomissioni malware. Il processo di avvio del BIOS utilizza la tecnologia Intel Boot Guard o AMD Root-of-Trust, in base alla quale la firma digitale dell'hash crittografico dell'immagine di avvio deve corrispondere alla firma archiviata nel silicio da Dell EMC in fabbrica.
Un errore nella verifica determina un arresto del server, una notifica all'utente nel registro di Lifecycle Controller e il processo di ripristino del BIOS può quindi essere avviato dall'utente. Se la convalida della funzione Boot Guard ha esito positivo, il resto dei moduli del BIOS viene convalidato utilizzando una catena di certificati finché il controllo non viene conferito al sistema operativo o all'hypervisor.

Oltre al meccanismo di verifica di Boot Guard, iDRAC9 4.10.10.10 o versioni successive fornisce un meccanismo di radice di affidabilità per verificare l'immagine del BIOS all'avvio dell'host. L'host può essere avviato solo dopo che l'immagine del BIOS è stata convalidata. iDRAC9 fornisce inoltre un meccanismo per convalidare l'immagine del BIOS in fase di esecuzione, on-demand o a intervalli pianificati dall'utente

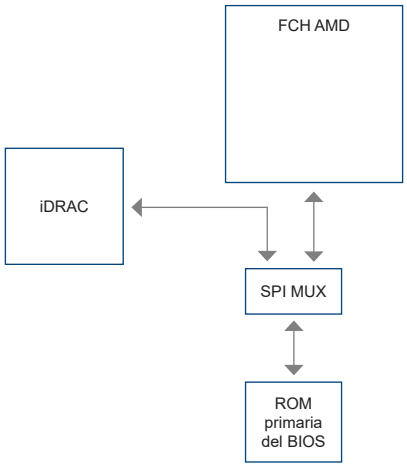
Analizziamo più a fondo la catena di affidabilità. Ciascun modulo del BIOS contiene un hash del modulo successivo nella catena. I moduli principali nel BIOS sono IBB (Initial Boot Block), SEC (Security), PEI (Pre-EFI Inizialization), MRC (Memory Reference Code), DXE (Driver Execution Environment) e BDS (Boot Device Selection). Se Intel Boot Guard autentica il modulo IBB (Initial boot Block), IBB convalida i moduli SEC e PEI prima di assegnarvi il controllo. SEC e PEI convalidano quindi PEI + MRC, che a loro volta convalidano i moduli DXE + BDS. A questo punto, il controllo viene trasferito a UEFI Secure Boot, come illustrato nella sezione successiva.

In modo analogo, per i server Dell EMC PowerEdge basati su AMD EPYC, la tecnologia AMD Secure Root-of-Trust garantisce l'avvio dei server solo da immagini del firmware affidabili. Inoltre, la tecnologia AMD Secure Run è progettata per crittografare la memoria principale, proteggendola da accessi di intrusi malevoli all'hardware. Non sono necessarie modifiche alle applicazioni per utilizzare questa funzione e il processore di sicurezza non espone mai le chiavi di crittografia all'esterno del processore.

Anche iDRAC assume il ruolo di tecnologia di sicurezza basata sull'hardware e accede alla ROM del BIOS primario tramite SPI, oltre che all'AMD FCH (Fusion Controller Hub), ed esegue il processo RoT.

Nelle condizioni riportate di seguito, iDRAC9 ripristina il BIOS.

1. Controllo dell'integrità del BIOS non riuscito.
2. Controllo automatico del BIOS non riuscito.
3. Utilizzo del comando RACADM - **racadm recover BIOS.Setup.1-1**



Il processo di avvio di iDRAC utilizza una Silicon Root of Trust indipendente che verifica l'immagine del firmware iDRAC. Anche iDRAC Root of Trust fornisce un punto di riferimento affidabile per l'autenticazione delle firme dei pacchetti di aggiornamento del firmware (DUP) di Dell EMC.

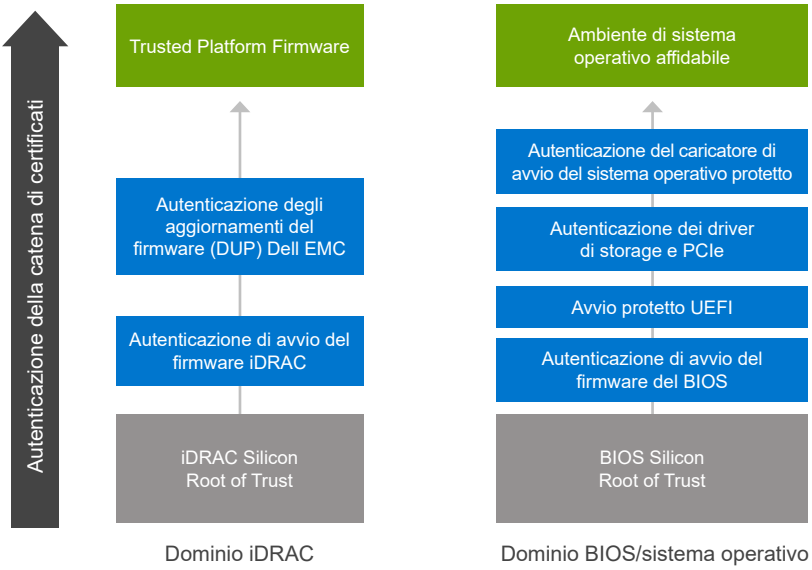


Figura 2: Domini Silicon Root of Trust nei server PowerEdge

3.1.2 BIOS Live Scanning

BIOS Live Scanning verifica l'integrità e l'autenticità dell'immagine del BIOS nella ROM primaria all'accensione dell'host, ma non durante il processo POST. Si tratta di una funzione esclusiva di AMD disponibile solo con iDRAC9 4.10.10.10 o versioni successive con licenza Datacenter. Per eseguire questa operazione, è necessario disporre di privilegi di amministratore o di operatore con privilegio di debug "Execute Debug Commands". È possibile pianificare la scansione tramite l'interfaccia utente di iDRAC e le interfacce RACADM e Redfish

3.1.3 Personalizzazione di UEFI Secure Boot

I server PowerEdge supportano inoltre la funzione UEFI (Unified Extensible Firmware Interface) Secure Boot standard del settore, che verifica le firme crittografiche dei driver UEFI e di altri codici caricati prima dell'esecuzione del sistema operativo. Secure Boot rappresenta uno standard di settore per la sicurezza nell'ambiente di preavvio. Fornitori di sistemi informatici, di schede di espansione e di sistemi operativi collaborano a questa specifica per promuovere l'interoperabilità.

Se abilitata, la funzione UEFI Secure Boot impedisce il caricamento dei driver di dispositivo UEFI senza firma, ovvero non affidabili, visualizza un messaggio di errore e blocca il funzionamento del dispositivo. È necessario disabilitare Secure Boot per caricare driver di dispositivo senza firma.

Inoltre, i server PowerEdge di 14ª e 15ª generazione garantiscono ai clienti la flessibilità esclusiva di utilizzare un certificato del caricatore di avvio personalizzato non firmato da Microsoft. Si tratta principalmente di una funzione per gli amministratori di ambienti Linux che intendono firmare i propri caricatori di avvio del sistema operativo. È possibile eseguire l'upload dei certificati personalizzati tramite l'API iDRAC preferita per autenticare il caricatore di avvio specifico del sistema operativo del cliente. Questo metodo di personalizzazione UEFI di PowerEdge viene citato dall' NSA per mitigare le vulnerabilità Grub2 nei server.

3.1.4 Supporto TPM

I server PowerEdge supportano tre versioni di TPM:

- TPM 1.2 FIPS + Common Criteria + TCG certified (Nuvoton)
- TPM 2.0 FIPS + Common Criteria + TCG certified (Nuvoton)
- TPM 2.0 China (NationZ)

Il modulo TPM può essere utilizzato per eseguire funzioni di crittografia a chiave pubblica, elaborare funzioni di hash, generare, gestire e archiviare in modo sicuro le chiavi ed eseguire l'attestazione. È inoltre supportata la funzionalità TXT (Trusted Execution Technology) di Intel insieme alla funzione Platform Assurance di Microsoft disponibile in Windows Server 2016. TPM può essere utilizzato anche per abilitare la funzione di crittografia del disco rigido BitLocker™ in Windows Server 2012/2016.

Le soluzioni di attestazione e attestazione remota possono utilizzare il modulo TPM per eseguire misurazioni in fase di avvio dell'hardware, dell'hypervisor, del BIOS e del sistema operativo di un server e confrontarle in modo sicuro a livello di crittografia con le misurazioni di base archiviate in TPM. Se non coincidono, l'identità del server potrebbe essere stata compromessa e i System Administrator possono disabilitare e disconnettere il server in locale o in remoto.

I server possono essere ordinati con o senza TPM, ma per molti sistemi operativi e altre disposizioni di sicurezza è ormai uno standard a tutti gli effetti. Il modulo TPM è abilitato tramite un'opzione del BIOS. Si tratta di una soluzione di modulo plug-in per cui il planare dispone di un connettore.

3.1.5 Certificazioni di sicurezza

Dell EMC ha ricevuto certificazioni per standard come NIST FIPS 140-2 e Common Criteria EAL-4, importanti per garantire la conformità alle direttive del Dipartimento di Difesa degli Stati Uniti e altri requisiti governativi. Sono state ricevute le seguenti certificazioni per i server PowerEdge:

- Piattaforma server: Certificazione Common Criteria EAL4+ con RHEL, anche per supportare le certificazioni CC partner
- Certificazione iDRAC e CMC FIPS 140-2 Level 1
- OpenManage Enterprise - Modular con certificazione EAL2+
- Certificazione FIPS 140-2 e Common Criteria per TPM 1.2 e 2.0

3.2 Sicurezza dell'accesso degli utenti

Garantire un livello appropriato di autenticazione e autorizzazione è un requisito fondamentale per qualsiasi policy moderna di controllo degli accessi. L'accesso per i server PowerEdge avviene tramite interfacce principali quali API, CLI o l'interfaccia grafica di iDRAC integrato. Le API e le CLI preferite per l'automazione della gestione dei server sono:

- API iDRAC RESTful con Redfish
- CLI RACADM
- SELinux

Ciascuna di esse fornisce credenziali affidabili, come la sicurezza di nome utente e password, trasportate su una connessione crittografata, ad esempio HTTPS. Il protocollo SSH autentica un utente mediante un set corrispondente di chiavi crittografiche (eliminando quindi la necessità di inserire password meno sicure). I protocolli meno recenti, come IPMI, sono supportati, ma non sono consigliati per le nuove implementazioni per via dei vari problemi di sicurezza individuati negli ultimi anni. Se attualmente si utilizza il protocollo IPMI, è consigliabile valutare e passare all'API RESTful iDRAC con Redfish.

È possibile eseguire l'upload dei **certificati TLS/SSL** su iDRAC per autenticare le sessioni del web browser. Tre opzioni:

- **Certificato TLS/SSL autofirmato di Dell EMC:** il certificato viene generato e firmato automaticamente da iDRAC.
  - » Advantage: non è necessario gestire un'autorità di certificazione distinta (vedere lo standard X.509/IETF PKIX).
- **Certificato TLS/SSL con firma personalizzata:** il certificato viene generato automaticamente e firmato con una chiave privata già sottoposta ad upload su iDRAC.
  - » Advantage: un'unica CA affidabile per tutti gli iDRAC. È possibile che la CA interna sia già affidabile per le stazioni di gestione.
- **Certificato TLS/SSL firmato dalla CA:** una richiesta di firma del certificato viene generata e inviata alla CA interna o a una CA di terze parti, come VeriSign, Thawte e Go Daddy, per la firma.
  - » Vantaggi: è possibile utilizzare un'autorità di certificazione commerciale (vedere gli standard X.509/IETF PKIX). Un'unica CA affidabile per tutti gli iDRAC. Se viene utilizzata una CA commerciale, è molto probabile che sia già affidabile per le stazioni di gestione.

iDRAC9 consente l'integrazione con **Active Directory** e **LDAP** sfruttando gli schemi di autenticazione e autorizzazione esistenti dei clienti che già garantiscono l'accesso protetto ai server PowerEdge. Supporta inoltre il **controllo degli accessi in base al ruolo** per garantire il livello di accesso adeguato, ovvero Administrator, Operator o Read Only, necessario per la corrispondenza del ruolo della persona nelle operazioni del server. Si consiglia vivamente di utilizzare il controllo degli accessi in base al ruolo in questo modo e non solo di concedere il livello più elevato (ad esempio, Administrator) a tutti gli utenti.

iDRAC9 fornisce inoltre metodi aggiuntivi per la protezione da accessi non autorizzati, tra cui il **blocco e il filtraggio IP**. Il blocco IP determina in modo dinamico quando si verificano errori di login non riuscito da un determinato indirizzo IP e blocca o impedisce all'indirizzo di accedere a iDRAC9 per un intervallo di tempo preselezionato. Il filtraggio IP limita l'intervallo di indirizzi IP dei client che accedono a iDRAC. Confronta l'indirizzo IP di un accesso in entrata con l'intervallo specificato e consente l'accesso a iDRAC solo da una stazione di gestione il cui indirizzo IP di origine si trova all'interno dell'intervallo. Tutte le altre richieste di accesso vengono negate.

L'**autenticazione a più fattori** è oggi più diffusa per via della crescente vulnerabilità degli schemi di autenticazione a fattore singolo basati su nome utente e password. iDRAC9 consente l'utilizzo di smart card per l'accesso remoto tramite interfaccia grafica utente e supporta inoltre il token RSA. In entrambi i casi, fattori multipli includono la presenza fisica di un dispositivo o di una scheda e il PIN associato.

3.2.1 Autenticazione a più fattori RSA SecurID

Anche RSA SecurID può essere utilizzato come strumento per l'autenticazione di un utente su un sistema. iDRAC9 inizia a supportare RSA SecurID con la licenza Datacenter e il firmware 4.40.00.00 come ulteriore metodo di autenticazione a due fattori.

3.2.2 Autenticazione a due fattori semplificata

Un altro metodo di autenticazione offerto è Easy 2FA, che invia un token generato casualmente all'indirizzo e-mail di un utente quando si esegue l'accesso a iDRAC.

3.2.3 Framework SELinux

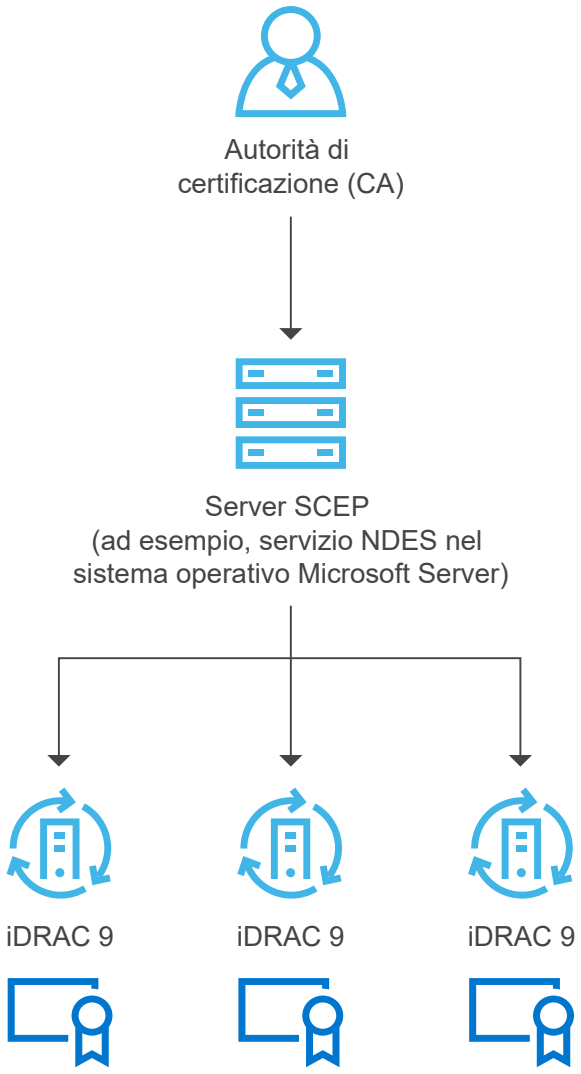
SELinux opera a livello di core kernel su iDRAC e non necessita di alcun input o configurazione da parte degli utenti. SELinux registra messaggi di sicurezza quando viene rilevato un attacco. I messaggi del registro indicano quando e come un utente malintenzionato ha tentato di accedere al sistema. Attualmente, questi registri sono disponibili tramite SupportAssist per i clienti iscritti a questa nuova funzione. In una versione futura di iDRAC questi registri saranno disponibili nei registri di Lifecycle Controller.

3.2.4 Privilegio minimo richiesto

Tutti i processi interni in esecuzione all'interno di iDRAC vengono eseguiti con i privilegi minimi richiesti, un concetto di sicurezza di base di UNIX. Questa protezione garantisce che il processo di un sistema che potrebbe essere attaccato non possa accedere ai file o all'hardware esterni all'ambito di tale processo. Ad esempio, il processo che fornisce il supporto per Virtual KVM non deve essere in grado di modificare la velocità delle ventole. L'esecuzione di questi due processi come funzioni distinte protegge il sistema impedendo la propagazione degli attacchi da un processo all'altro.

3.2.5 Iscrizione e rinnovo automatici dei certificati

iDRAC9 4.0 ha aggiunto un client per il supporto di Simple Certificate Enrollment Protocol (SCEP) e richiede la licenza Datacenter. SCEP è uno standard di protocollo utilizzato per la gestione dei certificati su un numero elevato di dispositivi di rete mediante un processo di iscrizione automatica. iDRAC può ora essere integrato con i server compatibili con SCEP, come il servizio Microsoft ServerNDES, per la gestione automatica dei certificati SSL/TLS. Questa funzione può essere utilizzata per l'iscrizione e l'aggiornamento di un certificato server web in scadenza e può essere eseguita individualmente nell'interfaccia grafica utente di iDRAC, impostata tramite Server Configuration Profile o convertita in script tramite strumenti come RACADM.



3.2.6 Password predefinita generata in fabbrica

Per impostazione predefinita, tutti i server PowerEdge 14G vengono forniti con una password iDRAC univoca generata in fabbrica per garantire maggiore sicurezza. Questa password si trova sull'etichetta informativa adesiva situata nella parte anteriore dello chassis, accanto all'etichetta del server. Gli utenti che scelgono questa opzione predefinita devono prendere nota di questa password e utilizzarla per effettuare l'accesso a iDRAC per la prima volta, anziché utilizzare una password predefinita universale. Per motivi di sicurezza, Dell EMC consiglia vivamente di modificare la password predefinita.

3.2.7 Dynamic System Lockdown

iDRAC9 offre una nuova funzionalità che "blocca" la configurazione dell'hardware e del firmware di uno o più server e richiede una licenza Enterprise o Datacenter. Questa modalità può essere abilitata mediante interfaccia grafica utente, CLI come RACADM oppure all'interno di Server Configuration Profile. Gli utenti con privilegi di amministratore possono impostare la modalità di blocco del sistema che impedisce l'esecuzione di modifiche al server da parte degli utenti con privilegi inferiori. Questa funzione può essere abilitata/disabilitata dall'amministratore IT. Le modifiche apportate quando il blocco del sistema è disabilitato vengono inserite nel registro di Lifecycle Controller. Abilitando la modalità di blocco, è possibile impedire deviazioni di configurazione nel data center quando si utilizzano strumenti e agenti di Dell EMC, oltre a garantire protezione da attacchi malevoli contro il firmware incorporato durante l'utilizzo di Dell EMC Update Packages. La modalità di blocco può essere abilitata in modo dinamico, senza dover riavviare il sistema. iDRAC9 4.40 introduce miglioramenti in cui, oltre all'attuale blocco del sistema, che controlla solo gli aggiornamenti tramite Dell Update Packages (DUP), questa funzionalità è estesa anche a determinate schede di rete. NOTA: la funzione di blocco avanzato per schede di rete include solo il blocco del firmware per impedirne gli aggiornamenti. Il blocco della configurazione (x-UEFI) non è supportato. Quando il cliente imposta il sistema in modalità di blocco abilitando/impostando l'attributo da qualsiasi interfaccia supportata, iDRAC intraprende le azioni aggiuntive in base alla configurazione del sistema. Queste azioni dipendono dai dispositivi di terze parti individuati nell'ambito del processo di rilevamento iDRAC.

3.2.8 Domain Isolation

i server PowerEdge di 14ª e 15ª generazione garantiscono un livello di sicurezza aggiuntivo grazie a **Domain Isolation**, una funzione importante per gli ambienti di hosting multi-tenant. Al fine di proteggere la configurazione hardware del server, gli hosting provider potrebbero bloccare eventuali riconfigurazioni da parte dei tenant. Domain Isolation è un'opzione di configurazione che garantisce che le applicazioni di gestione nel sistema operativo host non abbiano accesso a iDRAC fuori banda o alle funzioni del chipset Intel, come Management Engine (ME) o Innovation Engine (IE).

3.3 Aggiornamenti firmware firmati

Da varie generazioni i server PowerEdge utilizzano firme digitali sugli aggiornamenti del firmware per garantire che venga eseguito solo firmware autentico sulla piattaforma server. Firmiamo tutti i nostri pacchetti firmware in digitale mediante hashing SHA-256 con crittografia RSA a 2.048 bit per la firma di tutti i componenti principali del server, tra cui il firmware per iDRAC, BIOS, PERC, schede I/O e LOM, unità di alimentazione, unità di storage, CPLD e backplane controller. iDRAC cerca eventuali aggiornamenti del firmware e ne confronta le firme con il risultato previsto mediante Silicon Root of Trust. I pacchetti di firmware che non superano la convalida vengono interrotti e viene inserito un messaggio di errore nel registro di Lifecycle Controller per avvisare gli amministratori IT.

L'autenticazione del firmware migliorata è incorporata in molti dispositivi di terze parti che forniscono la convalida della firma utilizzando i propri meccanismi di radice di affidabilità. In questo modo si impedisce l'utilizzo di uno strumento di aggiornamento compromesso di terze parti per caricare firmware malevolo in una scheda di rete o un'unità di storage (e aggirare l'utilizzo di Dell EMC Update Packages firmati). Molti dispositivi di storage e PCIe di terze parti forniti con i server PowerEdge utilizzano una radice di affidabilità hardware per convalidare i rispettivi aggiornamenti del firmware.

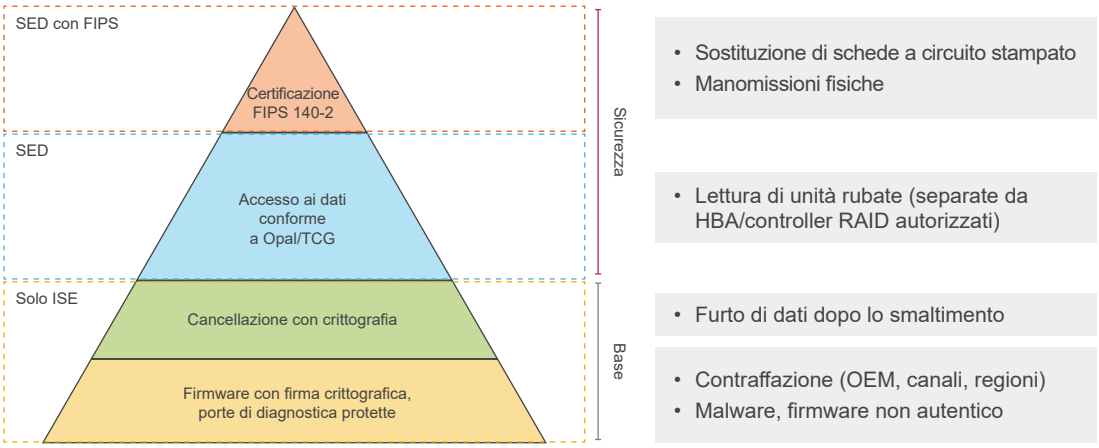
Se si sospetta che il firmware di un dispositivo sia stato manomesso, gli amministratori IT possono eseguire il rollback di molte delle immagini del firmware della piattaforma a una versione affidabile precedente archiviata in iDRAC. Conserviamo due versioni del firmware del dispositivo sul server, la versione di produzione esistente ("N") e una versione affidabile precedente ("N-1").

3.4 Storage dei dati crittografato

I server PowerEdge di 14ª e 15ª generazione offrono numerose unità di storage per la protezione dei dati. Come illustrato di seguito, le opzioni iniziano con unità che supportano Instant Secure Erase (ISE), una nuova tecnologia per cancellare i dati dell'utente in modo sicuro e immediato. I server di 14ª e 15ª generazione offrono unità compatibili con ISE per impostazione predefinita. La tecnologia ISE viene illustrata in dettaglio più avanti in questo documento all'interno della descrizione della funzione System Erase.

La successiva opzione di sicurezza avanzata è SED (Self-Encrypting Drive) che offre la protezione di blocco dell'unità di storage al server e alla scheda RAID utilizzata. In questo modo si evitano i cosiddetti furti "smash and grab" di unità e la conseguente perdita di dati sensibili degli utenti. Quando un ladro tenta di utilizzare l'unità, non conosce la passphrase del tasto di blocco richiesta e non può accedere ai dati dell'unità crittografata. I clienti possono evitare il furto dell'intero server mediante Secured Enterprise Key Manager (SEKM), funzione illustrata più avanti in questo documento.

Il livello di protezione più elevato è offerto dalle unità SED con certificazione NIST FIPS 140-2. Le unità conformi a questo standard sono state accreditate dai laboratori di test e dispongono di etichette adesive antimanomissione. Le unità SED Dell EMC dispongono di certificazione FIPS 140-2 per impostazione predefinita.



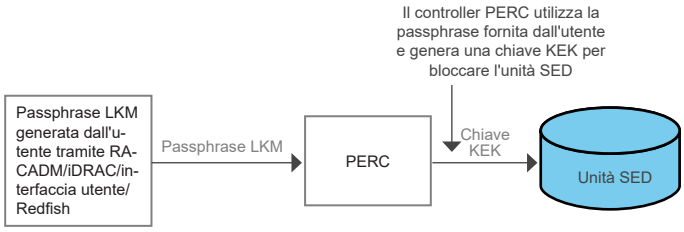
3.4.1 iDRAC Credential Vault

Il processore di servizio iDRAC fornisce una memoria di storage sicura che protegge vari dati sensibili come le credenziali utente e le chiavi private iDRAC per certificati SSL autofirmati. Ulteriore esempio di sicurezza basata sul silicio, questa memoria viene crittografata con una chiave radice non modificabile, programmata in ogni chip iDRAC al momento della produzione. Tutto questo garantisce una protezione dagli attacchi fisici in cui l'utente malintenzionato dissalda il chip nel tentativo di accedere ai dati.

3.4.2 Local Key Management (LKM)

I server PowerEdge attuali offrono agli utenti la possibilità di proteggere le unità SED collegate a un controller PERC mediante Local Key Management.

Per garantire la protezione dei dati dell'utente quando viene rubata un'unità, l'unità SED deve essere bloccata con una chiave distinta, in modo che non decrittografi i dati dell'utente, a meno che non venga fornita la chiave, detta Key Encryption Key (KEK). A tale scopo, un utente imposta una combinazione di keyId/passphrase sul controller PERC a cui è collegata l'unità SED e il controller PERC genera una chiave KEK utilizzando la passphrase e la impiega per bloccare l'unità SED. Ora, quando l'unità è accesa, viene visualizzata come un'unità SED bloccata e crittografa/decrittografa i dati dell'utente solo quando viene fornita la chiave KEK per sbloccarla. Il controller PERC fornisce la chiave KEK all'unità per sbloccarla, quindi se l'unità viene rubata appare come "bloccata" e, se l'utente malintenzionato non è in grado di fornire la chiave KEK, i dati dell'utente sono protetti. Questo processo include "local" nel nome in quanto la passphrase e la chiave KEK vengono archiviate in locale sul controller PERC.



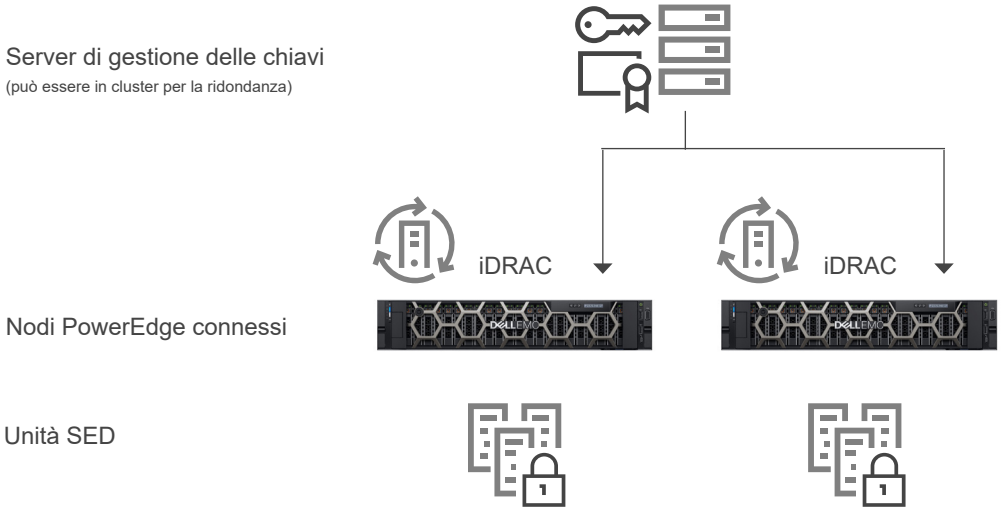
Nel diagramma riportato di seguito viene illustrata la soluzione LKM.

3.4.3 Secure Enterprise Key Manager (SEKM)

OpenManage SEKM offre una soluzione centralizzata di gestione delle chiavi per gestire i dati inattivi in tutta l'organizzazione. Consente al cliente di utilizzare un server di gestione delle chiavi esterno per gestire le chiavi che possono essere utilizzate da iDRAC per bloccare e sbloccare i dispositivi di storage su un server Dell EMC PowerEdge. Mediante l'uso di codice incorporato attivato con una licenza speciale, iDRAC richiede al server di gestione delle chiavi di creare una chiave per ciascun controller di storage, che viene recuperata e fornita al controller di storage a ogni avvio dell'host, in modo che il controller di storage possa sbloccare le unità SED.

I vantaggi dell'utilizzo di SEKM su Local Key Management (LKM) sono:

- Protezione contro il furto di un server, poiché le chiavi non sono archiviate nel server, ma esternamente, e vengono recuperate dai nodi dei server PowerEdge connessi (tramite iDRAC)
- Gestione delle chiavi centralizzata e scalabile per dispositivi crittografati con high availability
- Supporto del protocollo KMIP standard del settore, consentendo in tal modo l'utilizzo di altri dispositivi compatibili con KMIP
- Protezione dei dati inattivi in caso di danneggiamento delle unità o dell'intero server
- Scalabilità delle prestazioni di crittografia in base al numero di unità



3.5 Sicurezza hardware

La sicurezza hardware è parte integrante di una soluzione di sicurezza completa. Alcuni clienti desiderano limitare l'accesso alle porte di ingresso, ad esempio le porte USB. In generale, un server chassis non deve essere aperto dopo che è stato messo in produzione. In tutti i casi, i clienti intenderanno almeno monitorare e registrare queste attività. L'obiettivo generale è quello di scoraggiare e limitare le intrusioni fisiche.

3.5.1 Avviso di intrusione nello chassis

I server PowerEdge forniscono il rilevamento e la registrazione delle intrusioni nell'hardware; il rilevamento funziona anche in assenza di alimentazione CA. I sensori sullo chassis rilevano quando qualcuno apre o manomette lo chassis, anche durante il trasporto. Al collegamento dell'alimentazione, i server aperti durante il transito generano una voce nel log del ciclo di vita iDRAC.

3.5.2 Gestione dinamica delle porte USB

Per maggiore sicurezza, è possibile disabilitare completamente le porte USB. È inoltre possibile disabilitare solo le porte USB anteriori. Ad esempio, le porte USB possono essere disabilitate per l'uso in produzione e quindi temporaneamente abilitate per consentire l'accesso a un crash cart per scopi di debug.

3.5.3 iDRAC Direct

iDRAC Direct è una porta USB speciale sulla parte anteriore del server, cablata al processore di servizio iDRAC per il debug e la gestione nel server (corridoio freddo). Consente agli utenti di collegare un cavo USB standard Micro-AB a questa porta e l'altra estremità (Type-A) a un notebook. Un web browser standard può quindi accedere all'interfaccia utente di iDRAC per eseguire processi avanzati di debug e gestione del server. Se è installata la licenza iDRAC Enterprise, l'utente può anche accedere al desktop del sistema operativo tramite la funzione Virtual Console di iDRAC.

Poiché le normali credenziali iDRAC vengono utilizzate per l'accesso, iDRAC Direct funziona come un crash cart sicuro, con l'ulteriore vantaggio di una gestione hardware completa e della diagnostica dei servizi. Può risultare un'opzione interessante per proteggere l'accesso fisico al server in postazioni remote (le porte USB host e le uscite VGA possono essere disabilitate in questo caso).

3.5.4 iDRAC Connection View con geolocalizzazione

Connection View consente a iDRAC di segnalare gli switch e le porte esterni collegati all'I/O del server. Si tratta di una funzione disponibile su determinati dispositivi di rete che richiede l'abilitazione di LLDP (Link Layer Discovery Protocol) sugli switch collegati.

Di seguito sono riportati alcuni vantaggi associati a Connection View:

- Controllo rapido e in remoto per verificare se i moduli I/O del server (LOM, NDC e schede PCIe aggiuntive) sono connessi alle porte e agli switch corretti
- Risparmio evitando l'invio di tecnici per correggere errori di cablaggio
- Nessuna necessità di tracciare i cavi nei corridoi caldi della sala server
- Esecuzione tramite l'interfaccia grafica utente o ricezione di informazioni su tutte le connessioni 14G tramite comandi RACADM

Oltre all'ovvio risparmio di tempo e denaro, Connection View offre un ulteriore vantaggio, ovvero la geolocalizzazione in tempo reale di un server fisico o di una macchina virtuale. Mediante iDRAC Connection View, gli amministratori possono individuare un server per verificare esattamente lo switch e la porta a cui è collegato. In questo modo è possibile evitare che i server si connettano a reti e dispositivi non conformi alle best practice o alle linee guida di sicurezza aziendale.

Connection View convalida indirettamente la posizione del server segnalando le identità degli switch a cui è collegato. L'identità degli switch determina la geolocalizzazione e garantisce che non si tratti di un server non autorizzato in un sito non autorizzato, offrendo un ulteriore livello di sicurezza fisica. In questo modo si ottiene inoltre conferma del fatto che un'applicazione o una macchina virtuale non ha "attraversato" i confini del Paese e che è in esecuzione in un ambiente sicuro e approvato.

3.6 Integrità e sicurezza della supply chain

L'integrità della supply chain è incentrata su due sfide principali:

1. Mantenimento dell'integrità dell'hardware, per garantire che non si verifichino manomissioni o inserimenti di componenti contraffatti prima dell'invio di un prodotto a un cliente
2. Mantenimento dell'integrità del software, per garantire che non vengano inseriti malware nel firmware o nei driver dei dispositivi prima dell'invio di un prodotto a un cliente, oltre a impedire vulnerabilità del codice

Dell EMC definisce la sicurezza della supply chain come la prassi e l'applicazione di misure preventive e di controllo a protezione di asset fisici, inventario, informazioni, proprietà intellettuale e persone. Queste misure di sicurezza forniscono inoltre l'integrità e la garanzia della supply chain, riducendo i rischi di introduzione di malware e componenti contraffatti nella supply chain.

3.6.1 Integrità hardware e software

Dell EMC si impegna a garantire l'implementazione di processi di controllo della qualità per ridurre al minimo i rischi di introduzione di componenti contraffatti nella supply chain. I controlli messi in atto da Dell EMC riguardano la selezione dei fornitori, l'approvvigionamento, i processi di produzione e la governance attraverso procedure di verifica e test. Una volta selezionato un fornitore, il processo di introduzione di un nuovo prodotto verifica che tutti i materiali utilizzati in tutte le fasi di creazione vengano ricavati dall'elenco dei fornitori approvati e corrispondano alla distinta materiali in base alle esigenze. Le ispezioni dei materiali durante la produzione identificano i componenti che sono contrassegnati in modo errato, si discostano dai normali parametri delle prestazioni o contengono un ID elettronico non corretto.

Laddove possibile, le parti vengono acquistate direttamente dall'ODM (Original Design Manufacturer) o dall'OCM (Original Component Manufacturer) originale. L'ispezione dei materiali che si verifica durante il processo di introduzione di un nuovo prodotto offre diverse opportunità per identificare componenti contraffatti o danneggiati che potrebbero essere stati inseriti nella supply chain.

Inoltre, Dell EMC 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 EMC o che nel firmware o nei driver dei dispositivi vengano inseriti malware. Queste misure vengono implementate nell'ambito del processo SDL (Software Development Lifecycle).

3.6.2 Sicurezza fisica

Dell EMC include tre pratiche chiave di lunga data che stabiliscono e garantiscono la sicurezza negli impianti di produzione e nelle reti logistiche. Ad esempio, abbiamo bisogno di determinati stabilimenti in cui i prodotti Dell EMC vengano realizzati per soddisfare i requisiti di sicurezza degli impianti TAPA (Transported Asset Protection Association), tra cui l'utilizzo di telecamere a circuito chiuso monitorate in aree chiave, controllo degli accessi e ingressi e uscite continuamente sorvegliati. Sono state inoltre adottate misure speciali per proteggere i prodotti da furti e manomissioni durante il trasporto nell'ambito di un programma logistico leader del settore. Questo programma fornisce un centro di comando con personale disponibile 24 ore su 24 per monitorare la selezione delle spedizioni in entrata e in uscita in tutto il mondo al fine di garantire che i prodotti giungano a destinazione senza interruzioni.

Dell EMC è inoltre attivamente impegnata in vari programmi e iniziative di volontariato sulla sicurezza della supply chain. Una di queste iniziative è il C-TPAT (Customs-Trade Partnership Against Terrorism), una certificazione introdotta dal governo degli Stati Uniti dopo l'11 settembre per ridurre il potenziale di attacchi terroristici attraverso il rafforzamento delle misure di sicurezza dei confini e della supply chain. Nell'ambito di questa iniziativa, l'ente delle dogane e della polizia di frontiera degli Stati (U.S. Customs and Border Protection) chiede ai membri partecipanti di garantire l'integrità delle loro prassi di sicurezza e di comunicare le loro linee guida di sicurezza ai business partner all'interno della supply chain. Dell EMC partecipa attivamente all'iniziativa dal 2002 con status di membro più elevato.

3.6.3 Dell Technologies Secured Component Verification (SCV) per PowerEdge

Dell Technologies Secured Component Verification (SCV) è un'offerta di garanzia per la supply chain che consente ai clienti Dell EMC di verificare che un server PowerEdge ricevuto dal cliente corrisponda al prodotto realizzato in fabbrica. Al fine di convalidare i componenti in un modo sicuro a livello di crittografia, durante il processo di produzione viene generato un certificato in fabbrica contenente ID di componenti univoci per un server specifico. Questo certificato viene firmato in fabbrica da Dell Technologies, archiviato in iDRAC e successivamente utilizzato dal cliente nell'applicazione SCV. Il cliente utilizza l'applicazione SCV per raccogliere l'inventario del sistema corrente, inclusi gli ID di componenti univoci, e lo convalida in base all'inventario nel certificato SCV.

Il report generato dall'applicazione SCV verifica i componenti corrispondenti e quelli che si discostano dalle parti installate in fabbrica. Verifica inoltre il certificato e la catena di affidabilità, unitamente alla prova di possesso della chiave privata SCV per iDRAC. L'implementazione attuale supporta i clienti con spedizione diretta e non include rivenditori a valore aggiunto (VAR) o scenari di sostituzione di componenti.

4. Rilevamento

È essenziale disporre di una funzionalità di rilevamento che garantisca una visibilità completa sulla configurazione, sullo stato di integrità e sugli eventi di modifica all'interno di un sistema server. Questa visibilità deve inoltre rilevare modifiche dannose o di altro tipo al BIOS, al firmware e alle ROM opzionali all'interno del processo di avvio e di runtime del sistema operativo. Il polling proattivo deve essere abbinato alla possibilità di inviare avvisi per tutti gli eventi all'interno del sistema. I registri devono fornire informazioni complete sull'accesso e sulle modifiche al server. Il server, infine, deve soprattutto estendere queste funzionalità a tutti i componenti.

4.1 Monitoraggio completo tramite iDRAC

Anziché dipendere dagli agenti del sistema operativo per comunicare con le risorse gestite in un server, iDRAC utilizza un percorso a banda laterale diretto per ciascun dispositivo. Dell EMC utilizza protocolli standard del settore, come MCTP, NC-SI e NVMe-MI, per comunicare con periferiche quali controller RAID PERC, schede di rete Ethernet, HBA fibre channel, HBA SAS e unità NVMe. Questa architettura è il risultato di partnership pluriennali con fornitori leader del settore volte a fornire una gestione dei dispositivi senza agente nei server PowerEdge. Le operazioni di configurazione e aggiornamento del firmware sfruttano inoltre le potenti funzioni UEFI e HII supportate da Dell EMC e dai nostri partner.

Con questa funzionalità, iDRAC è in grado di monitorare eventi di configurazione, eventi di intrusione (come il rilevamento delle intrusioni nello chassis menzionato in precedenza nel presente documento) e modifiche di stato nel sistema. Gli eventi di configurazione sono direttamente associati all'identità dell'utente che ha avviato la modifica, che si tratti di un utente dell'interfaccia grafica, di un'API o della console.

4.1.1 Registro del ciclo di vita

Il registro del ciclo di vita è una raccolta di eventi che si verificano in un server in un determinato periodo di tempo. Il registro del ciclo di vita fornisce una descrizione degli eventi con data e ora, il livello di gravità, l'ID utente o l'origine, le azioni consigliate e altre informazioni tecniche che potrebbero rivelarsi estremamente utili ai fini del monitoraggio o dell'invio di avvisi.

Di seguito sono riportati i vari tipi di informazioni archiviate nel registro del ciclo di vita:

- Modifiche alla configurazione sui componenti hardware del sistema
- Modifiche alla configurazione di iDRAC, BIOS, schede di rete e RAID
- Registri di tutte le operazioni remote
- Cronologia degli aggiornamenti del firmware in base a dispositivo, versione e data
- Informazioni sulle parti sostituite
- Informazioni sulle parti guaste
- ID di eventi e messaggi di errore
- Eventi relativi all'alimentazione dell'host
- Errori del processo POST
- Eventi di accesso degli utenti
- Eventi di modifica degli stati dei sensori

4.1.2 Avvisi

iDRAC offre la possibilità di configurare avvisi di eventi diversi, nonché le azioni da eseguire quando si verifica un determinato evento di registro del ciclo di vita. Quando viene generato un evento, questo viene inoltrato alle destinazioni configurate utilizzando i meccanismi selezionati del tipo di avviso. È possibile abilitare o disabilitare gli avvisi tramite l'interfaccia web di iDRAC, i comandi RACADM o l'utilità di configurazione di iDRAC.

iDRAC supporta vari tipi di avvisi, tra cui:

- Avviso e-mail o IPMI
- trap SNMP
- Registri dell'OS e dei sistemi remoti
- Evento Redfish

Gli avvisi possono inoltre essere classificati in base al livello di gravità: Critical, Warning oppure Informational.

I seguenti filtri possono essere applicati agli avvisi:

- System health, ad esempio errori di temperatura, tensione o dispositivo
- Storage health, ad esempio errori del controller, del disco fisico o del disco virtuale
- Configuration changes, ad esempio modifica della configurazione RAID o rimozione della scheda PCIe
- Audit logs, ad esempio errore di autenticazione tramite password
- Firmware/Driver, ad esempio upgrade o downgrade

Infine, l'amministratore IT può impostare diverse azioni per gli avvisi: Reboot, Power Cycle, Power Off oppure No action.

4.2 Rilevamento delle deviazioni

Con l'applicazione di configurazioni standardizzate e l'adozione di una policy di tolleranza zero per qualsiasi modifica, le organizzazioni possono ridurre il potenziale di sfruttamento. La console Dell EMC OpenManage Enterprise consente al cliente di definire la propria baseline di configurazione server e quindi di monitorare la deviazione dei server di produzione da tale baseline. La baseline può essere creata in base a criteri diversi per soddisfare l'applicazione di produzioni differenti, ad esempio la sicurezza e le prestazioni. OpenManage Enterprise è in grado di segnalare eventuali deviazioni dalla baseline e, come opzione facoltativa, di riparare la deviazione con un flusso di lavoro semplice per eseguire le modifiche su iDRAC fuori banda. Le modifiche possono quindi essere eseguite nelle finestre di manutenzione successive durante il riavvio dei server per garantire nuovamente la conformità dell'ambiente di produzione. Questo processo per fasi consente al cliente di implementare modifiche alla configurazione in produzione senza downtime del server al di fuori delle ore di manutenzione. Aumenta la disponibilità del server senza compromettere la facilità di manutenzione o la sicurezza.

5. Ripristino

Le soluzioni server devono supportare il ripristino a uno stato noto e coerente in risposta a una varietà di eventi:

- Nuove vulnerabilità individuate
- Attacchi dannosi e manomissioni dei dati
- Danneggiamento del firmware a causa di errori della memoria o procedure di aggiornamento non corrette
- Sostituzione dei componenti del server
- Ritiro o ridestinazione di un server

Di seguito sono indicate in dettaglio le modalità in cui rispondiamo alle nuove vulnerabilità e ai problemi di danneggiamento e le procedure con cui ripristiniamo lo stato originale dei server, se necessario.

5.1 Risposta rapida a nuove vulnerabilità

Gli eventi CVE (Common Vulnerabilities and Exposures, vulnerabilità ed esposizioni comuni) sono nuovi vettori di attacco che compromettono i prodotti software e hardware. Risposte tempestive a eventi CVE sono fondamentali per la maggior parte delle aziende per poter valutare rapidamente la loro esposizione e intraprendere azioni appropriate.

Possono essere generati eventi CVE in risposta a nuove vulnerabilità identificate in molti elementi, tra cui:

- Codice open source, ad esempio OpenSSL
- Web browser e altri prodotti software di accesso a Internet
- Hardware e firmware di prodotti di fornitori
- Sistemi operativi e hypervisor

Dell EMC si impegna in modo efficace per rispondere rapidamente a nuovi eventi CVE nei server PowerEdge e per fornire ai clienti informazioni tempestive, tra cui:

- Prodotti interessati
- Potenziali operazioni correttive
- Se necessario, data di disponibilità degli aggiornamenti per risolvere uno specifico evento CVE

5.2 Ripristino del BIOS e del sistema operativo

I server Dell EMC PowerEdge di 14ª e 15ª generazione includono due tipi di ripristino: Ripristino del BIOS e ripristino rapido dell'OS. Queste funzioni consentono il ripristino rapido dalle immagini danneggiate del BIOS o dell'OS. In entrambi i casi, uno store speciale è nascosto dal software di run-time (BIOS, OS, firmware del dispositivo, ecc.). Questi store contengono immagini incontaminate che possono essere utilizzate come alternative al software principale compromesso.

Il ripristino rapido del sistema operativo consente il ripristino rapido da un'immagine del sistema operativo danneggiata (o un'immagine del sistema operativo potenzialmente manomessa). I supporti di ripristino includono schede SD interne, porte SATA, unità M.2 o porte USB interne. Il dispositivo selezionato può essere esposto all'elenco di avvio e al sistema operativo per l'installazione dell'immagine di ripristino. Può quindi essere disabilitato e nascosto dall'elenco di avvio e dal sistema operativo. Nello stato nascosto, il BIOS disabilita il dispositivo in modo che non sia accessibile dal sistema operativo. Nel caso di un'immagine del sistema operativo danneggiata, il percorso di ripristino può essere quindi abilitato per l'avvio. È possibile accedere a queste impostazioni tramite il BIOS o l'interfaccia di iDRAC.

In casi estremi, se il BIOS è danneggiato (a causa di un attacco dannoso, un'interruzione dell'alimentazione durante il processo di aggiornamento o qualsiasi altro evento imprevisto), è importante fornire un metodo per ripristinare lo stato originale del BIOS. Un'immagine del BIOS di backup viene archiviata in iDRAC in modo che possa essere utilizzata per ripristinare l'immagine del BIOS, se necessario. iDRAC coordina l'intero processo di ripristino end-to-end.

- Il ripristino automatico del BIOS viene avviato dal BIOS stesso.
- Il ripristino del BIOS on-demand può essere avviato dagli utenti utilizzando il comando della CLI RACADM.

5.3 Rollback del firmware

Si consiglia di mantenere aggiornato il firmware per disporre delle funzioni e degli aggiornamenti di sicurezza più recenti. Potrebbe tuttavia essere necessario eseguire il rollback di un aggiornamento o installare una versione precedente se si verificano problemi dopo un aggiornamento. Se si esegue il rollback alla versione precedente, viene anche verificata la firma.

Il rollback del firmware dalla versione di produzione esistente "N" a una versione precedente "N-1" è attualmente supportato per le seguenti immagini del firmware:

- BIOS
- iDRAC con Lifecycle Controller
- Scheda di interfaccia di rete
- Controller RAID PowerEdge (PERC)
- Alimentatore (PSU)
- Backplane

È possibile eseguire il rollback del firmware alla versione precedentemente installata ("N-1") utilizzando uno dei seguenti metodi:

- Interfaccia web di iDRAC
- Interfaccia web di CMC
- CLI RACADM - iDRAC e CMC
- Interfaccia grafica utente di Lifecycle Controller
- Lifecycle Controller - Remote Services

È possibile eseguire il rollback del firmware per iDRAC o qualsiasi dispositivo supportato da Lifecycle Controller, anche se l'aggiornamento è stato eseguito in precedenza utilizzando un'altra interfaccia. Se ad esempio il firmware è stato aggiornato utilizzando l'interfaccia grafica utente di Lifecycle Controller, è possibile eseguire il rollback del firmware utilizzando l'interfaccia web di iDRAC. È possibile eseguire il rollback del firmware per più dispositivi con un solo riavvio del sistema.

Nei server PowerEdge di 14ª e 15ª generazione con un unico firmware per iDRAC e Lifecycle Controller, il rollback del firmware iDRAC esegue anche il rollback del firmware di Lifecycle Controller.

5.4 Ripristino della configurazione server dopo la manutenzione dell'hardware

La correzione degli eventi di assistenza è un elemento fondamentale di qualsiasi operazione IT. La capacità di soddisfare i Recovery Time Objective e i Recovery Point Objective ha ripercussioni dirette sulla sicurezza della soluzione. Il ripristino della configurazione server e del firmware garantisce il rispetto automatico delle policy di sicurezza per il funzionamento del server.

I server PowerEdge forniscono funzionalità per il ripristino rapido della configurazione server nelle seguenti situazioni:

- Sostituzione di componenti individuali
- Sostituzione della scheda madre (backup e ripristino del profilo server completo)
- Sostituzione della scheda madre (Easy Restore)

5.4.1 Sostituzione dei componenti

iDRAC salva automaticamente l'immagine del firmware e le impostazioni di configurazione per le schede di rete, i controller RAID e le unità di alimentazione. In caso di sostituzione sul campo di queste parti, iDRAC rileva automaticamente la nuova scheda e ripristina il firmware e la configurazione nella scheda sostituita. Questa funzionalità consente di risparmiare tempo essenziale e garantisce una configurazione e una policy di sicurezza coerenti. L'aggiornamento avviene automaticamente al riavvio del sistema dopo la sostituzione della parte supportata.

5.4.2 Easy Restore (per la sostituzione della scheda madre)

La sostituzione della scheda madre può richiedere molto tempo e influire sulla produttività. iDRAC offre la possibilità di eseguire il backup e il ripristino della configurazione e del firmware di un server PowerEdge per ridurre al minimo lo sforzo necessario per la sostituzione di una scheda madre guasta.

Esistono due modi in cui il server PowerEdge può eseguire il backup e il ripristino:

1. I server PowerEdge effettuano automaticamente il backup delle impostazioni di configurazione del sistema (BIOS, iDRAC, scheda di rete), del codice di matricola, dell'app di diagnostica UEFI e di altri dati concessi in licenza nella memoria flash.

   Dopo aver sostituito la scheda madre sul server, Easy Restore richiede di ripristinare automaticamente i dati.
2. Per un risultato più completo, un utente può eseguire il backup della configurazione del sistema, includendo le immagini del firmware installate su vari componenti, come BIOS, RAID, scheda di rete, iDRAC, Lifecycle Controller e schede di rete secondarie, e delle impostazioni di configurazione di questi componenti. L'operazione di backup include inoltre i dati di configurazione del disco rigido, la scheda madre e le parti sostituite. Il backup crea un singolo file che è possibile salvare in una scheda SD vFlash o in una share di rete (CIFS, NFS, HTTP o HTTPS).

   Questo backup di profilo può essere ripristinato in qualsiasi momento dall'utente. Dell EMC consiglia di eseguire l'operazione di backup per ciascun profilo di sistema che si ritiene possa essere necessario ripristinare in un determinato momento.

5.5 System Erase

Al termine del ciclo di vita di un sistema, è necessario ritirarlo o riutilizzarlo. L'obiettivo di System Erase consiste nella cancellazione delle impostazioni e dei dati sensibili dai dispositivi di storage e dagli archivi non volatili del server, come le cache e i registri, in modo che non vengano inavvertitamente divulgate informazioni riservate. Si tratta di un'utilità in Lifecycle Controller progettata per cancellare i registri, i dati di configurazione, i dati di storage, la memoria cache e tutte le applicazioni integrate.

I seguenti dispositivi, impostazioni di configurazione e app possono essere cancellati utilizzando la funzione di cancellazione del sistema:

- iDRAC viene reimpostato su predefinito
- Dati di Lifecycle Controller (LC)
- BIOS
- Sistemi di diagnostica integrati e pacchetti di driver dell'OS
- iSM
- Rapporti sulla raccolta SupportAssist

È inoltre possibile cancellare i seguenti componenti:

- Cache dell'hardware (cancellazione di PERC NVCache)
- Scheda SD vFlash (scheda di inizializzazione) (nota: vFlash non è disponibile sui server 15G o versioni successive).

I dati sui seguenti componenti vengono cancellati in modo crittografico da System Erase come descritto di seguito:

- Unità SED (Self-Encrypting Drive)
- Unità solo ISE (Instant Secure Erase)
- Dispositivi NVM (Apache Pass, NVDIMM)

Inoltre, i dischi rigidi SATA non ISE possono essere cancellati mediante sovrascrittura dei dati.

Si noti che Instant Secure Erase (ISE) elimina la chiave di crittografia interna utilizzata nelle unità di 14ª e 15ª generazione, rendendo quindi irrecuperabili i dati dell'utente. ISE è un metodo riconosciuto di erasure dei dati sulle unità di storage a cui si fa riferimento nella Pubblicazione speciale NIST 800-88 "Linee guida per la sanificazione dei supporti".

I vantaggi della nuova funzione ISE con System Erase sono i seguenti:

- **Velocità:** molto più veloce rispetto alle tecniche di sovrascrittura dei dati, come DoD 5220.22-M (secondi anziché ore)
- **Efficacia:** ISE rende completamente illeggibili tutti i dati presenti sull'unità, inclusi i blocchi riservati
- **TCO superiore:** i dispositivi di storage possono essere riutilizzati anziché smaltiti o fisicamente distrutti

È possibile eseguire System Erase tramite i seguenti metodi:

- Interfaccia grafica utente di Lifecycle Controller (F10)
- CLI RACADM
- Redfish

5.6 iDRAC9 Cipher Select

È possibile utilizzare Cipher Suite Selection per limitare le crittografie che il web browser può utilizzare per comunicare con iDRAC. Consente inoltre di determinare il grado di sicurezza della connessione. Queste impostazioni possono essere configurate tramite l'interfaccia web di iDRAC, RACADM e Redfish. Questa funzionalità è disponibile in diverse versioni di iDRAC: iDRAC7, iDRAC8 (2.60.60.60 e versioni successive) e l'attuale iDRAC9 (3.30.30.30 e versioni successive).

5.7 Supporto CNSA

Di seguito sono riportate le crittografie supportate disponibili in iDRAC9 con TLS 1.2 e crittografia a 256 bit.
Le crittografie disponibili includono quelle presenti nel set approvato da CNSA.

5.8 Ciclo di alimentazione completo

In un ciclo di alimentazione completo vengono riavviati il server e tutti i relativi componenti. Il ciclo scarica l'alimentazione principale e ausiliaria dal server e da tutti i componenti. Vengono cancellati anche tutti i dati presenti nella memoria volatile.

In un ciclo di alimentazione fisico completo è necessario estrarre il cavo di alimentazione CA, attendere 30 secondi e quindi reinserire il cavo, il che rappresenta un problema quando si lavora con un sistema remoto. Una nuova funzione nei server 14G e 15G consente di eseguire un efficace ciclo di alimentazione completo da iSM, dall'interfaccia grafica utente di IDRAC, dal BIOS o con uno script. Il ciclo di alimentazione completo ha effetto al successivo ciclo di alimentazione.

Questa funzione elimina la necessità di essere fisicamente presenti nel data center, riducendo così i tempi di risoluzione dei problemi. Permette ad esempio di eliminare eventuali malware ancora presenti nella memoria.

6. Riepilogo

La sicurezza dei data center è fondamentale per il successo aziendale e la sicurezza dell'infrastruttura server sottostante è di importanza critica. Gli attacchi informatici possono comportare downtime estesi dei sistemi e dell'azienda, perdita di entrate e clienti, danni legali e alla reputazione aziendale. Per garantire la protezione, il rilevamento e il ripristino da attacchi informatici mirati all'hardware, la sicurezza deve essere integrata nella progettazione dell'hardware del server, non aggiunta in un secondo momento.

Dell EMC è leader nell'utilizzo di un livello di sicurezza basata sul silicio per proteggere il firmware e i dati sensibili degli utenti nei server PowerEdge delle ultime due generazioni. Le linee di prodotti PowerEdge di 14ª e 15ª generazione sono caratterizzate da un'architettura cyber-resiliente migliorata che rafforza ulteriormente la sicurezza dei server mediante Silicon Root of Trust, incluse le seguenti funzioni:

- **Avvio protetto verificato tramite crittografia**, che stabilizza la sicurezza del server end-to-end e la sicurezza complessiva del data center. Include funzioni come Silicon Root of Trust, il firmware con firma digitale e il ripristino automatico del BIOS
- **Secure Boot**, che verifica le firme crittografiche dei driver UEFI e altro codice caricato prima dell'esecuzione del sistema operativo.
- **iDRAC Credential Vault**, uno spazio di storage protetto per credenziali, certificati e altri dati sensibili crittografati con una chiave basata sul silicio univoca per ogni server
- **Dynamic System Lockdown,** una funzionalità esclusiva di PowerEdge che protegge qualsiasi configurazione di sistema e firmware da modifiche dannose o non intenzionali con l'invio di avvisi all'utente in merito a tentativi di modifiche nel sistema
- **Enterprise Key Management**, una soluzione centralizzata di gestione delle chiavi per gestire i dati inattivi in tutta l'organizzazione.
- **System Erase**, che consente agli utenti di ritirare o ridestinare facilmente i server PowerEdge di 14ª e 15ª generazione grazie alla cancellazione sicura e rapida dei dati dalle unità di storage e da altre non-volatile memory integrate
- La **sicurezza della supply chain** fornisce la garanzia della supply chain evitando che si verifichino manomissioni o inserimenti di componenti contraffatti prima dell'invio di un prodotto al cliente.

In conclusione, i server PowerEdge di 14ª e 15ª generazione, con la loro sicurezza leader del settore, costituiscono una base affidabile per l'IT Transformation su cui i clienti eseguono in modo sicuro le operazioni e i carichi di lavoro IT.

A. Appendice: altre letture

White paper sulla sicurezza e materiale informativo

- (Direct from Development) SYSTEM ERASE SUI SERVER POWEREDGE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242
- SECURING 14TH GENERATION DELL EMC POWEREDGE SERVERS WITH SYSTEM ERASE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- (Direct from Development) SECURITY IN SERVER DESIGN
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243
- (Direct from Development) CYBER-RESILIENCY IN CHIPSET AND BIOS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- PASSWORD PREDEFINITA DI IDRAC9 GENERATA IN FABBRICA
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368
- DELL EMC IDRAC RESPONSE TO CVE-2017-1000251 "BLUEBORNE"
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605
- (Video) SECURE BOOT CONFIGURATION AND CERTIFICATE MANAGEMENT USING RACADM
  https://youtu.be/mrIIN4X380c
- SECURE BOOT MANAGEMENT ON DELL EMC POWEREDGE SERVERS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- Signing UEFI images for Secure Boot feature in the 14th and 15th generation and later Dell EMC PowerEdge servers
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255
- RAPID OPERATING SYSTEM RECOVERY
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- Managing iDRAC9 Event Alerts on 14th generation (14G) Dell EMC PowerEdge Servers
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266
- UEFI Secure Boot Customization
  https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

White paper su PowerEdge

- Panoramica di iDRAC
  http://www.DellTechCenter.com/iDRAC
- Panoramica della console OpenManage
  http://www.DellTechCenter.com/OME
- Panoramica di OpenManage Mobile
  http://www.DellTechCenter.com/OMM
- Sostituzione di componenti Lifecycle Controller
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- Sostituzione della scheda madre
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- iDRAC Automatic Certificate Enrollment
  https://www.dellemc.com/resources/it-it/asset/white-papers/products/software/direct-from-development-idrac-automatic-certificate-enrollment.pdf
- Improved Server Security with iDRAC9 and SELinux
  https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_en-us.pdf
- iDRAC9 Cipher Select - Improved Security for Dell EMC PowerEdge Servers
  https://downloads.dell.com/manuals/all-products/esuprt_software_int/esuprt_software_ent_systems_mgmt/idrac9-lifecycle-controller-v33-series_white-papers11_en-us.pdf

Scopri di più sui server PowerEdge

Scopri di più sui nostri server Dell PowerEdge.

Scopri di più sulle nostre soluzioni di gestione dei sistemi

Cerca nella nostra libreria di risorse

Segui i server PowerEdge su Twitter

Contatta un esperto Dell Technologies per le vendite o il supporto

DELL Technologies