DELL Technologies

Breve panoramica sulla soluzione

Personalizzazione dell'avvio protetto UEFI di Dell EMC PowerEdge

Gli ambienti server data center tradizionalmente si concentrato principalmente sulle attività di sicurezza a livello di sistema operativo, applicazioni e rete. Man mano che i problemi legati alla sicurezza dell'infrastruttura hardware continuano ad aumentare, cresce anche la complessità per i Security Administrator IT. Un'esigenza fondamentale per team IT di server e sicurezza è creare una base di elaborazione affidabile ed estendere tale affidabilità ai sistemi operativi e alle applicazioni. Solitamente riservata alle applicazioni e ai dataset più protetti e sensibili, la sicurezza dell'infrastruttura personalizzata sta rapidamente venendo alla ribalta. La minaccia in continua evoluzione per l'hardware del server richiede un approccio più completo, inclusa la personalizzazione dell'avvio protetto UEFI, per rafforzare questa base affidabile.

Inizia dall'architettura Dell EMC cyber-resiliente, che convalida il BIOS e il firmware per l'Integrated Dell Remote Access Controller (iDRAC) prima che venga caricato. Il firmware per altri componenti critici è convalidato in modo analogo utilizzando certificati crittografici archiviati per garantire che sul server sia in esecuzione un firmware autentico.

Architettura Dell EMC cyber-resiliente

Protezione efficace

- Radice di affidabilità hardware basata su silicio
- Aggiornamenti firmware firmati
- Blocco del sistema
- Password predefinite protette

Rilevamento affidabile

- Rilevamento delle deviazioni a livello di configurazione e firmware
- Registrazione eventi persistente, compresa l'attività dell'utente
- Avvisi protetti

Ripristino rapido

- Ripristino automatico del BIOS
- Ripristino rapido del sistema operativo
- System Erase

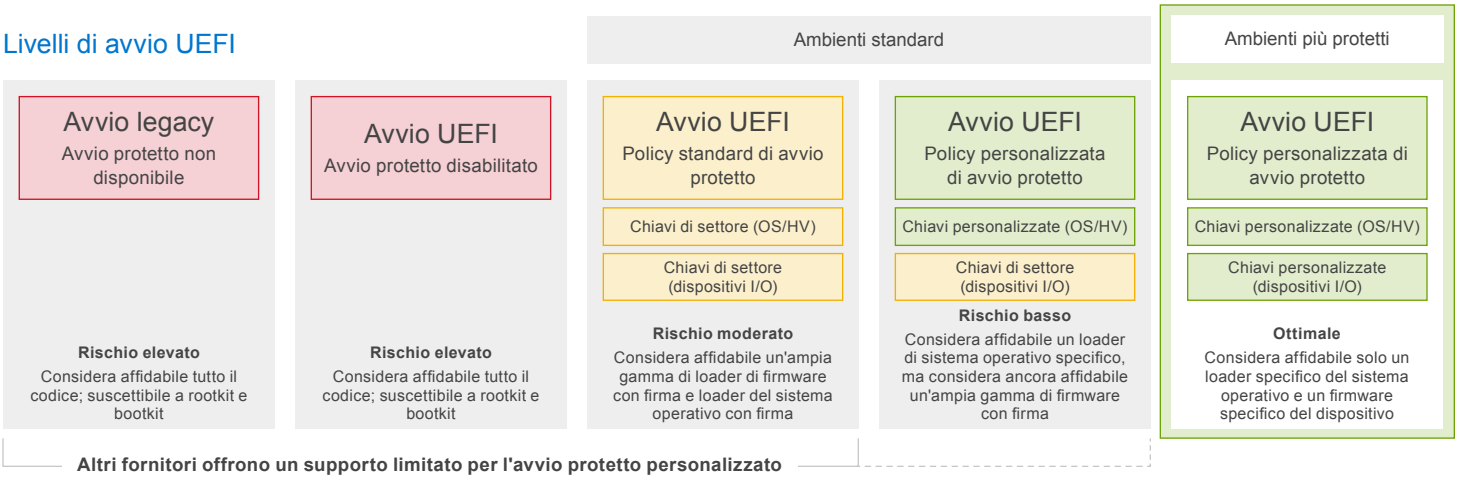
Come funzionalità sostitutiva moderna della configurazione del BIOS e dei controlli di avvio legacy, l'avvio protetto UEFI inizializza le funzioni di base del server prima che venga avviato un hypervisor o un sistema operativo. I server PowerEdge utilizzano l'avvio protetto UEFI per verificare i certificati generati crittograficamente dai driver UEFI e dai boot loader del sistema operativo. Queste sono le "chiavi" che consentono al server di convalidare:

- Driver UEFI caricati da schede PCIe
- Driver UEFI e file eseguibili caricati da dispositivi di storage di massa
- Boot loader del sistema operativo: in genere Linux o Microsoft Windows

Questo processo di convalida è fondamentale per proteggere il server dall'avvio di codice non autorizzato prima dell'avvio del sistema operativo. Controllando la firma del boot loader, del kernel e di altro codice di spazio utente, la convalida del firmware UEFI è progettata per impedire l'esecuzione di software senza firma sul sistema.

La personalizzazione dell'avvio protetto UEFI di Dell EMC PowerEdge dispone anche della capacità esclusiva di supportare certificati personalizzati generati e firmati da un'autorità diversa da Microsoft. Microsoft è l'autorità di certificazione predefinita per dispositivi e sistemi operativi supportati da UEFI. Molte distribuzioni Linux standard hanno implementato un certificato Microsoft. Nelle situazioni in cui viene utilizzato un ambiente Linux non standard (ad esempio, le modifiche del kernel o dei driver proprietari) è necessario disporre di certificati generati in modo personalizzato, firmati con crittografia dall'utente, per convalidare autonomamente il boot loader e mantenere la catena di affidabilità da hardware a software.

Livelli di avvio UEFI



Miglioramenti apportati alla sicurezza del server senza compromessi

Il processo di avvio costituisce la base per la sicurezza di qualsiasi dispositivo. Si basa su una moltitudine di firmware che controlla il modo in cui vengono avviati componenti e periferiche di un dispositivo, nonché il caricamento del sistema operativo. Il codice precedente viene caricato, più è privilegiato e maggiore è il danno che può fare se non viene autenticato prima. Se il processo di avvio è compromesso, gli autori di attacchi informatici possono sovvertire i controlli di sicurezza, ottenendo un accesso non autorizzato a varie parti del sistema. È anche possibile creare ransomware utilizzando boot loader UEFI dannosi per assumere il controllo dei server al momento dell'avvio, riconfigurando il computer, crittografando i dati e causando caos.

Ridurre i rischi

Grazie a moderne opzioni di controllo e configurazione, è più che mai possibile proteggere i server dagli attacchi di firmware o boot loader. La personalizzazione dell'avvio protetto UEFI di Dell EMC PowerEdge aumenta la sicurezza dell'infrastruttura server lasciandosi alle spalle i metodi di avvio legacy basati su BIOS. Un recente consiglio dell'NSA (National Security Agency) del Governo degli Stati Uniti tratta l'argomento di una maggiore sicurezza hardware del server, citando espressamente l'uso della personalizzazione dell'avvio protetto UEFI di PowerEdge come metodo che fornisce un livello di sicurezza significativamente più elevato, insieme alla flessibilità necessaria per supportare più sistemi operativi. In un report tecnico sulla sicurezza informatica della NSA, si nota che "la modalità personalizzata consente al proprietario del sistema di limitare o ampliare la selezione di soluzioni hardware e software affidabili..." e illustra come questa operazione può essere eseguita utilizzando l'utility di configurazione UEFI incorporata in Dell[1]. Questo controllo granulare può ridurre o eliminare la minaccia di errata configurazione, manomissione e malware. I System Administrator possono reagire più rapidamente alle nuove minacce di avvio e sono isolati da potenziali errori di firma dei certificati creati dai fornitori.

Funzioni di avvio protetto UEFI con certificati personalizzati

Funzioni	Descrizione	Vantaggi
Avvio protetto	• Convalida di componenti chiave e firmware	• Adozione di una moderna convalida del firmware, lasciandosi alle spalle limitazioni e minacce alla sicurezza del BIOS legacy
Certificati Self-Signed	• Garanzia di protezione per firmware, boot loader e avvio del sistema operativo durante l'intero ciclo d'uso del server	• Supporto di build del sistema operativo personalizzate in installazioni altamente protette • Indipendenza dall'autorità di firma predefinita durante l'implementazione di hardware incorporato personalizzato e firmware associato
Conformità a linee guida per la sicurezza	• Allineamento agli standard di sicurezza per processo di avvio del server, convalida del firmware e gestione personalizzata di certificati	• Impostazione dello standard per la sicurezza del firmware e dell'hardware del server • Posizionamento di operazioni del server per la conformità alle linee guida future sulla sicurezza dei server in ambienti sensibili
Integrazione con iDRAC e TPM	• Uso di funzionalità di protezione del firmware e dell'hardware esistenti già integrate con server PowerEdge	• Massimizzazione del valore delle funzioni di sicurezza integrate per stabilire una radice di affidabilità hardware completa

[1] Come per la maggior parte delle impostazioni di sistema, un amministratore può utilizzare altri strumenti oltre all'installazione del sistema per abilitare la policy standard di avvio protetto. DTK (Deployment Toolkit™) di Dell, Lifecycle Controller™, strumenti OpenManage™, console RACADM e console WS-MAN possono anche abilitare la policy standard di avvio protetto.

Scopri di più sui server PowerEdge

Scopri di più su Dell EMC OpenManage Enterprise

Scopri di più sulle nostre soluzioni di gestione dei sistemi

Cerca nella nostra libreria di risorse

Segui server PowerEdge su Twitter

Contatta un esperto Dell Technologies per le vendite o il supporto