
DELL Technologies
intel
Resilienza informatica
Contrasta le minacce con un approccio alla sicurezza in profondità che inizia con i server Dell PowerEdge, basati su processori scalabili Intel® Xeon®.
Inizia

Sommario

Cliccare sulle icone o sui titoli dei capitoli riportati di seguito per accedere a sezioni specifiche. Utilizzare i pulsanti freccia in alto per spostarsi da una pagina all'altra. Utilizzare il pulsante Home nell'angolo in alto a sinistra per tornare all'inizio.

Parte 1: il panorama della sicurezza informatica

Minacce sempre in evoluzione

Le minacce e gli attacchi informatici stanno diventando sempre più nefasti e diffusi e, soprattutto, se ne prevede un aumento. Nel 2020, Cybersecurity Ventures ha previsto una crescita dei costi globali per il contrasto alla criminalità informatica del 15% all'anno nei prossimi cinque anni, arrivando così a toccare il valore di 10,5 trilioni di dollari all'anno entro il 2025, rispetto ai 3 trilioni di dollari del 2015.[1] Dal momento che si accede ai dati da più dispositivi, sia on-premise sia su cloud, le violazioni dei dati a impatto elevato continuano ad aumentare. Per mantenere un ambiente più sicuro, le aziende devono adottare un approccio più completo.

Negli anni 2000 la Digital Transformation è stato l'argomento di conversazione principale, negli anni 2020 se ne parla ancora di più, in quanto le organizzazioni si sforzano di adattarsi ad ambienti aziendali nuovi e in rapida evoluzione. Con un'adozione più diffusa dei Software-Defined Data Center (SDDC), le organizzazioni sono diventate più dipendenti dai server come elemento fondamentale per le funzioni aziendali. Ciò significa che la sicurezza dei server deve essere fondamentale per la strategia di difesa aziendale complessiva, proteggendo dalle minacce fino al livello del firmware.

Sfide per la sicurezza informatica

Le minacce informatiche stanno arrivando alle aziende da tutti i livelli. Gli attori tradizionali includono hacktivisti, gruppi terroristici, stati-nazione ostili, organizzazioni criminali, hacker individuali e spie industriali, ma sempre più si deve essere diffidenti nei confronti delle minacce interne.

Le notizie di oggi si concentrano sull'aumento della velocità, della sofisticazione, dell'efficacia e dell'impatto finanziario degli attacchi informatici. Ad esempio, nel 2021 è stato riscontrato il 50% in più a settimana di attacchi informatici sulle reti aziendali rispetto al 2020.[2] E sebbene il ransomware sia costato al mondo 20 miliardi di dollari nel 2021, tale valore aumenterà fino a 265 miliardi di dollari entro il 2031.[3]

Si prevede che entro il 2031 gli attacchi ransomware costeranno al mondo

265 miliardi di dollari.[3]

[1] CyberCrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 13 novembre 2020

[2] DARKReading, Businesses Suffered 50% More Cyberattack Attempts per Week in 2021, 11 gennaio 2022.

[3] Cloudwards, Ransomware Statistics, Trends, and Facts for 2022 and Beyond, 22 marzo 2022.

Gli attacchi più comuni includono:

Malware: include qualsiasi software malevole come spyware, adware o virus che può danneggiare le prestazioni o la sicurezza del server.

Ransomware: il ransomware è una forma di software o malware dannoso che, una volta scaricato su un server, può bloccare l'accesso a dati e file sul dispositivo fino a quando non viene pagato un riscatto.

Attacchi phish o phishing: il phishing è l'atto di contattare fraudolentemente più persone o aziende nel tentativo di ottenere l'accesso non autorizzato a informazioni sensibili e/o personali.

Supply chain: queste sono situazioni in cui gli hacker cercano sempre più di sfruttare i punti deboli della supply chain o vendor di terze parti, in quanto la sicurezza di tutte le organizzazioni è sempre più elevata. L'attacco informatico del 2020 accaduto a SolarWinds, una delle principali società di gestione IT, è passato inosservato per mesi, il che ha consentito a SolarWinds di infettare inconsapevolmente i propri clienti con un codice dannoso. Secondo Accenture, "il 40% degli attacchi informatici mira a colpire la supply chain".[4]

Il 40%
degli attacchi informatici mira a colpire la supply chain.[4]

[4] Accenture, Securing the Supply Chain, 2020

Conformità e pressione normativa

Con l'aumento delle minacce globali, continuano a verificarsi pressioni normative volte a definire linee guida sulle best practice per la protezione non solo delle infrastrutture critiche e della pubblica amministrazione, ma anche del settore privato. È significativo perché, negli Stati Uniti, quasi il 90% dell'infrastruttura critica, come il settore sanitario, energetico, finanziario, dei trasporti, delle telecomunicazioni e delle utility, è di proprietà del settore privato.[5]

Nei mesi di maggio 2021 e gennaio 2022, gli Stati Uniti hanno emesso degli ordini esecutivi della Casa Bianca che hanno delineato un framework per la protezione dell'infrastruttura nazionale, oltre a fornire indicazioni dettagliate sull'architettura Zero Trust. Gli Stati Uniti non sono però l'unico Paese ad agire. I governi internazionali stanno sviluppando linee guida normative in risposta alle minacce informatiche e gli istituti privati stanno approntando policy e normative per ridurre le minacce persistenti avanzate. Questi requisiti vanno ben oltre le agenzie federali, raggiungendo l'infrastruttura critica e altri mercati verticali.

Mentre i governi cercano di colpire o ridurre al minimo gli attacchi informatici, le organizzazioni si aspettano un numero maggiore di linee guida e mandati come:

- **Autenticazione a più fattori (MFA):** MFA, nota anche come autenticazione a due fattori (2FA),[6] protegge dall'accesso ai dati da terze parti non autorizzate. Si tratta di una tecnologia di sicurezza per cui un utente, per ottenere l'accesso, deve fornire due o più credenziali indipendenti. I settori che includono "finanza, sanità, difesa, forze dell'ordine e governo federale richiedono già l'autenticazione a due fattori per accedere a sistemi, reti, siti web e sedi di edifici fisici".[7]
- **Crittografia dei dati inattivi**: self-encrypting drive con attività di gestione principali di livello enterprise

[5] La Casa Bianca, Press Briefing: Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure, 28 luglio 2021.
[6] NIST, Back to Basics: What's multi-factor authentication - and why should I care?, 16 giugno 2016.
[7] Okta, Which Industries Require Two-Factor Authentication?, consultato nel giugno 2022.

Cosa c'è in gioco?

Gli attacchi informatici possono essere devastanti per un'organizzazione. A seconda della portata dell'attacco e dei danni provocati, il tempo di ripristino può essere notevole. In media, sono necessari 22 giorni per il ripristino da un attacco ransomware.[8] Sfide che le organizzazioni possono trovarsi ad affrontare:

- Downtime per tentare di scoprire cosa è successo e ripristinare la perdita di eventuali dati
- Perdita permanente dei dati interni e dei clienti, con conseguente compromissione a lungo termine dei prospect
- Pagamento di multe e retrofit per garantire la conformità a tutte le regole e normative
- Pubblicità negativa e perdita di profitto nell'immediato dopo un attacco informatico
- Danno alla reputazione a lungo termine in quanto i clienti sono restii a continuare ad affidarsi ad aziende vittime di attacchi informatici

Richiede, in media,
22 giorni
per il ripristino da un attacco ransomware.[8]

Alcune organizzazioni sono così concentrate sulla crescita del business che potrebbero trascurare le misure di sicurezza appropriate per proteggere e sostenere le attività. Tuttavia, una violazione può incidere rapidamente nell'organizzazione aziendale. Se a questo si unisce il fatto che l'infrastruttura, i carichi di lavoro e l'utilizzo dei dati stanno diventando sempre più complessi, il risultato è che la manutenzione di un'infrastruttura e l'esecuzione di operazioni IT sicure sono diventate molto più complicate.

Se da un lato la Digital Transformation crea opportunità illimitate, dall'altro le sfide associate alla creazione di un ambiente IT agile e moderno, mantenendo al contempo la fiducia dei clienti e delle entità interessate, permangono. Se non si riesce a stare al passo con le crescenti minacce alla sicurezza, i danni possono essere catastrofici. Una lezione da tenere a mente è che il 64% degli americani avrebbe dato la colpa della perdita dei propri dati personali in occasione di un attacco informatico all'azienda anziché all'hacker.[9] Inoltre, l'84% dei consumer ha confermato di essere più fedele nei confronti di aziende considerate più affidabili in termini di controlli di sicurezza.[10]

[8] Statista, Length of impact after a ransomware attack Q1 2020- Q3 2021, novembre 2021.
[9] Forbes, 50 Stats Showing Why Companies Need To Prioritize Consumer Privacy, 22 giugno 2020.
[10] Report di ricerca SalesForce, State of the Connected Customer: Terza edizione, giugno 2019.

Risorse

Infografica Cyber Resilient Architecture

Video Cyber Resilient Architecture

Documento tecnico Cyber Resilient Security in Dell PowerEdge Servers

Parte 2: best practice del settore

Zero Trust

è un approccio architettonico costituito da un framework di principi di sicurezza e best practice.

Zero Trust risponde alla complessità degli ambienti IT moderni, tra cui il cloud e l'hybrid cloud, asset basati su cloud che non si trovano all'interno del limite di rete dell'organizzazione. A complicare il tutto si aggiunge anche il recente aumento degli utenti remoti, di milioni di dispositivi personali (Bring-Your-Own-Device, BYOD) e di altre normative governative.

Zero Trust non è una singola architettura, ma un insieme di principi guida per il flusso di lavoro, la progettazione del sistema e le operazioni. Gli approcci a una sicurezza efficace si sono evoluti da un set statico e poco sofisticato di perimetri in qualcosa di molto più fluido, in cui non viene concessa alcuna fiducia agli asset o agli account utente esclusivamente in base alla propria posizione fisica o al percorso di rete o alla proprietà degli asset.

In altre parole, un approccio Zero Trust valuta e convalida numerosi punti nell'ambiente IT prima di concedere le autorizzazioni. L'elemento cruciale dello Zero Trust è la verifica degli asset all'interno dell'azienda prima di fornire l'accesso e la verifica continua prima dell'esecuzione del processo o dello spostamento laterale all'interno della rete.

Risorse

Infografica Zero-trust architecture

La pressione normativa è aumentata in modo significativo dopo il successo degli attacchi ransomware che hanno colpito le entità federali, l'infrastruttura critica e il settore privato. Un esempio è dato dall'ordine esecutivo della Casa Bianca emesso il 12 maggio 2021. Da allora, sono stati creati molti documenti che illustrano i dettagli per l'implementazione della sicurezza e le nuove normative. Dal momento che le linee guida normative continuano a evolversi, le organizzazioni che si stanno adoperando per trovare soluzioni per la sicurezza sono diventate la norma e non più una rarità. I requisiti Zero Trust a partire da SP800-207 con il Dipartimento della Difesa degli Stati Uniti hanno continuato a essere definiti insieme all'ordine esecutivo della Casa Bianca e in collaborazione con l'unità CISA e OMB. Stiamo notando che i governi internazionali seguono l'esempio con requisiti più rigorosi in tutto il mondo.[11]

[11] NIST, Zero Trust Architecture, 10 agosto 2020.

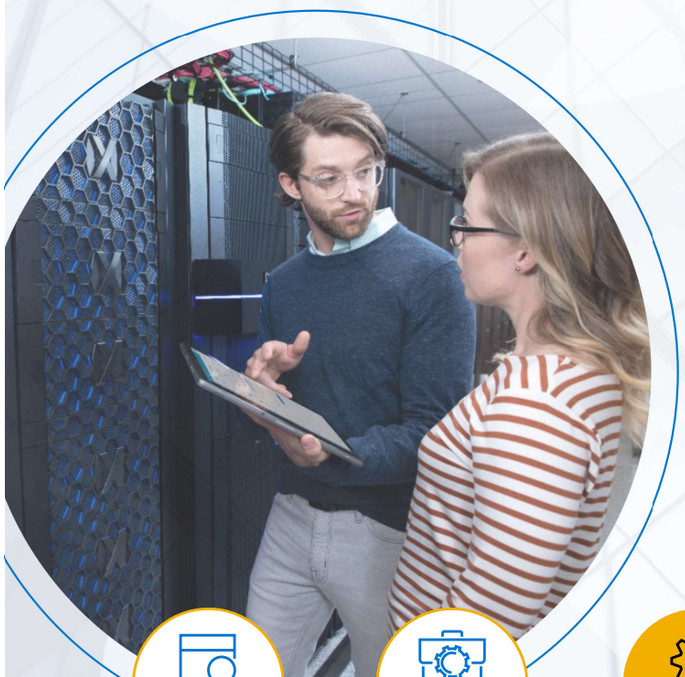
Parte 3: iniziare da una base sicura

La filosofia di Dell per la sicurezza risiede nella nostra cyber-resilienza.

La creazione di una cyber-resilienza efficace inizia con una vision di protezione delle organizzazioni da malintenzionati durante tutto il ciclo di vita delle apparecchiature. In linea con il NIST Cybersecurity framework, Dell si affida a un approccio del ciclo di vita dello sviluppo della sicurezza (SDL) (NIST SP800-160) per creare prodotti e soluzioni che comprendono le esigenze di sicurezza dalla progettazione, produzione, supply chain e gestione alla dismissione.

- Il firmware del server è progettato in modo da bloccare, ostacolare e contrastare l'introduzione di codici dannosi durante tutte le fasi del ciclo di vita dello sviluppo del prodotto.
- Vengono applicate procedure di codifica sicure in ogni fase dello sviluppo del firmware.
- Copertura dei test di penetrazione e modellazione delle minacce durante il processo di progettazione.

La tutela dei dati e della proprietà intellettuale richiede un approccio a più livelli. Nei server Dell PowerEdge, le funzionalità di protezione sono progettate intenzionalmente con livelli sovrapposti per cui, se un meccanismo viene compromesso, è presente un altro livello che contrasta l'attacco. Questo approccio di "difesa in profondità" fornisce una migliore resilienza ed è al centro della nostra architettura resiliente agli attacchi informatici.



I server PowerEdge sono basati su processori scalabili Intel Xeon che offrono funzionalità di sicurezza avanzate tra cui Intel SGX, che aiuta a proteggere i dati e il codice delle applicazioni in tempo reale dall'edge al data center e al public cloud multi-tenant. Ciò consente una collaborazione migliorata (ad esempio per l'apprendimento federato nell'intelligenza artificiale) utilizzando dati condivisi, senza compromettere la privacy. Intel Crypto Acceleration aumenta le prestazioni dei carichi di lavoro a uso intensivo di crittografia tra cui web serving SSL, infrastruttura 5G e VPN/firewall e riduce l'impatto sulle prestazioni della crittografia pervasiva.

Questa architettura si basa su una legacy di sicurezza PowerEdge con funzionalità avanzate che proteggono efficacemente l'infrastruttura rilevando in modo affidabile le minacce e ripristinando rapidamente in caso di attacchi informatici. Si tratta di un approccio allineato ai componenti chiave di NIST Framework (NIST SP 800-193).

Radice di affidabilità basata su silicio

I server PowerEdge utilizzano una radice di affidabilità basata su silicio immutabile per confermare crittograficamente l'integrità del BIOS e del firmware iDRAC (Integrated Dell Remote Access Controller). Questa radice di affidabilità si basa su chiavi pubbliche one-time programmabili e read-only che garantiscono la protezione contro le manomissioni malware. Uno degli aspetti più critici della sicurezza dei server consiste nel garantire che il processo di avvio possa essere verificato come sicuro. La radice di affidabilità fornisce un punto di ancoraggio affidabile per le operazioni di avvio. In aggiunta, il processo di avvio del BIOS sfrutta la tecnologia Intel Boot Guard che verifica che la firma digitale dell'hash crittografico dell'immagine di avvio corrisponda alla firma archiviata nel silicio da Dell Technologies in fabbrica.

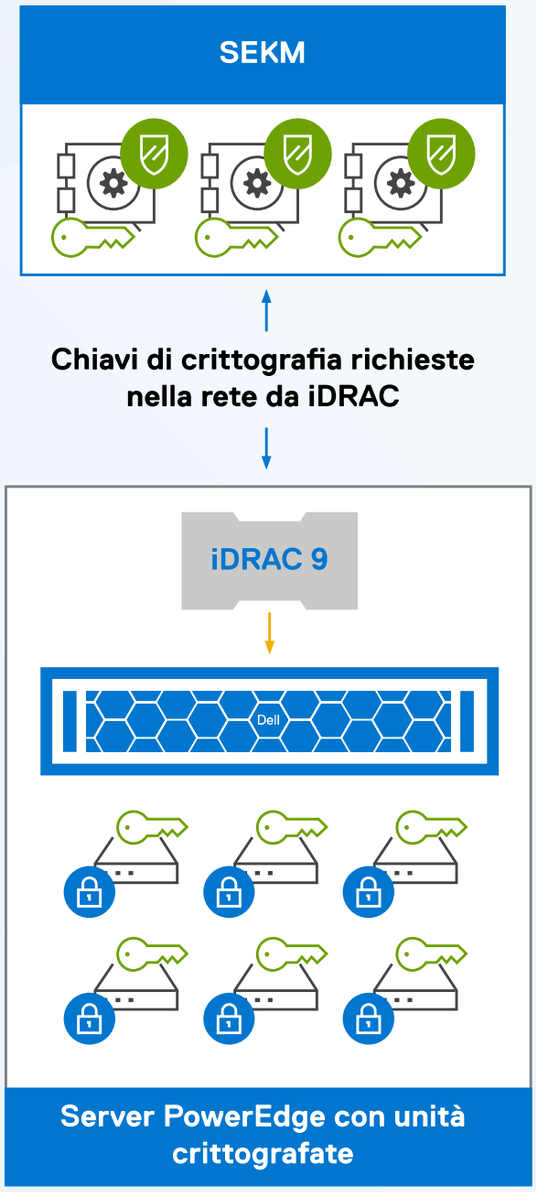
Identity and Access Management

La gestione degli accessi e delle identità (IAM) è un'area critica in particolare per la protezione contro gli attacchi ransomware con controlli come l'MFA per abilitare i privilegi minimi e un approccio orientato allo Zero Trust in ambito di sicurezza. L'IAM è progettata per garantire che solo determinate persone possano accedere agli asset e ai dati IT appropriati e controllare l'ambito di accesso.

Protezione dei dati avanzata

La protezione dei dati prevede la protezione dei dati aziendali, indipendentemente dal fatto che siano in uso, in transito o at-rest, in genere tramite crittografia. I server PowerEdge offrono un'ampia gamma di opzioni di storage sicuro per i dati.

La gestione delle chiavi esterne è una best practice in cui le chiavi vengono memorizzate lontano dalle unità e dal server di hosting. Secure Enterprise Key Manager (SEKM) consente ai clienti PowerEdge di gestire le chiavi in modo centralizzato per le unità autocrittografanti nei server PowerEdge ed è scalabile con l'espansione della capacità di storage. La gestione locale delle chiavi (LKM) è disponibile anche per gli ambienti in cui l'accesso centrale potrebbe essere difficile o in cui i requisiti di sicurezza sono meno rigorosi.



Esempio di implementazione SEKM

Risorse

Infografica Data Protection

Pagina web SEKM

Video SEKM

Documento tecnico Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell PowerEdge Servers

Infografica SEKM

Video Cyber Resilient Architecture

Ciclo di vita dello sviluppo della sicurezza Dell

Dell Technologies crea volontariamente il codice di controllo di sicurezza per ogni fase del ciclo di vita del server, dalla raccolta dei requisiti alla manutenzione del server. Ciò include il codice sviluppato per ostruire, bloccare e contrastare l'introduzione.

Panorama sulla sicurezza informatica

Best practice del settore

Supporto del framework NIST

Modello Zero Trust

Il successo dell'azienda

Garanzia della supply chain verificata

L'approccio completo di Dell Technologies a protezione della supply chain include disposizioni fondamentali come il personale fisico e i controlli di sicurezza informatica. Dell Technologies migliora inoltre la garanzia di integrità dei componenti con l'offerta SCV (Secured Component Verification). SCV consente ai clienti di verificare crittograficamente che i componenti impostati in fabbrica corrispondano a quanto è stato consegnato loro.

Sicurezza fornisce la riservatezza, l'integrità e la disponibilità delle informazioni che descrivono la supply chain IT o che attraversano la supply chain IT, nonché informazioni sulle parti che partecipano alla supply chain IT.

Integrità garantisce che i prodotti o i servizi IT nella supply chain IT siano originali e inalterati e che vengano eseguiti in base alle specifiche dell'acquirente e senza ulteriori funzionalità indesiderate.

Qualità riduce le vulnerabilità che possono limitare la funzione di un componente, portare a guasti o fornire opportunità di utilizzo.

Resilienza garantisce che la supply chain IT fornisca i prodotti e i servizi IT necessari nonostante le interruzioni.

Risorse

Video Secured Component Verification

Nota tecnica Secured Component Verification

Discussione tecnica Secured Component Verification

Gruppo NCC: Documento tecnico relativo alla supply chain Secured Component Verification Security Assessment

Vantaggi dei prodotti cyber-resilienti

- Uptime massimo per la produttività del personale
- Conservazione della reputazione dell'azienda
- Fiducia dei clienti
- Conformità per evitare costose sanzioni e retrofit
- Libertà di innovare senza distrazioni

Parte 4: utilizzo della cyber-resilienza per soddisfare i requisiti Zero Trust

L'approccio Zero Trust di Dell Technologies è stato ottimizzato per allinearsi agli U.S. Department of Defense (DoD) standards. Consentiamo un'architettura Zero Trust attraverso ampie funzionalità di resilienza informatica nei confronti di minacce informatiche e un approccio a sette pilastri che consente agli utenti di verificare in ogni momento nell'ambiente IT prima che le autorizzazioni vengano concesse.

Pilastro 1: affidabilità del dispositivo

La nostra radice di affidabilità hardware basata su silicio fornisce un livello di sicurezza per l'intero ciclo di vita dei server, dalla progettazione alla dismissione. La nostra supply chain sicura include più livelli di controllo, come la component verification, per garantire che i nostri server e software non siano stati manomessi o modificati in modo malevolo. SCV offre certificati di inventario con firma crittografica in tutto il portafoglio di server PowerEdge, inclusa l'auto-verifica sicura, in modo da ottenere la tranquillità dell'integrità dell'hardware durante il trasporto verso il data center.

Pilastro 2: fiducia degli utenti

Con iDRAC, gli amministratori IT possono implementare, aggiornare e monitorare in modo sicuro i server PowerEdge in locale o in remoto. Per migliorare la sicurezza, iDRAC offre l'MFA utilizzando RSA SecureID anche con integrazioni tramite Active Directory, l'integrazione LDAP con Single Sign-On (SSO) e con controllo e verifica degli accessi basati sui ruoli.

Pilastro 3: affidabilità di trasporto e sessione

PowerEdge BMC (iDRAC) dispone di un modulo di rete dedicato e le opzioni Secure Shell (SSH)/Transport Layer Security (TLS) funzionano per crittografare e autenticare i dati che passano tra i server e il browser che esegue l'interfaccia utente web di iDRAC. iDRAC consente la gestione remota e monitora il sistema per gli eventi critici utilizzando i sensori sulla scheda di sistema. Gli avvisi e gli eventi di registro vengono inviati quando i parametri superano le soglie presenti.

Pilastro 4: affidabilità del software

Eseguiamo test proattivi di verifica, convalida e sicurezza durante tutto il ciclo di vita del software per salvaguardare il nostro software e ridurre la probabilità che vengano inserite vulnerabilità di malware o codici. L'avvio verificato end-to-end include immagini del BIOS e del firmware con firma, che garantiscono che il codice non autorizzato non venga eseguito su un server PowerEdge. Altre funzionalità cyber-resilienti includono il rilevamento automatico delle discrepanze, le funzionalità di avvio UEFI protette e il ripristino per BIOS e sistemi operativi.

Pilastro 5: fiducia nei dati

SEKM funziona insieme alle self-encrypting drive per la crittografia basata su hardware e alle attività di gestione principali scalabili per facilitare l'implementazione e il monitoraggio delle chiavi di crittografia, incluse le posizioni remote e anche nel cloud. Ciò fornisce protezione contro l'accesso non autorizzato a unità o sistemi persi o rubati. Questa crittografia hardware può essere combinata con la crittografia software come la crittografia VMware® vSAN™ su VxRail.

L'elaborazione riservata consente la protezione dei dati in uso su CPU e memoria e include le tecnologie Intel (SGX, TME). Intel SGX fornisce isolamento a livello di applicazione o funzione per ridurre al minimo il perimetro di attendibilità.

La combinazione della crittografia di dati inattivi, attività di gestione principali scalabili ed elaborazione riservata può offrire i livelli di protezione necessari per contrastare le attuali minacce in continua evoluzione.

Pilastro 6: visibilità e analisi

La possibilità di osservare gli eventi che si verificano nell'ambiente è fondamentale. Il rilevamento delle deviazioni del firmware, ad esempio, fornisce informazioni dettagliate in tempo reale sullo stato del firmware, incluse eventuali modifiche non autorizzate. Se vengono rilevate modifiche, il sistema può essere riportato a uno stato sicuro noto. È inoltre possibile tenere traccia degli eventi di modifica tramite la registrazione automatizzata e gli avvisi, che supporteranno l'audit e l'analisi per valutare lo stato generale del sistema.

Pilastro 7: automazione e orchestration

OpenManage Enterprise è un'applicazione di gestione e monitoraggio dei sistemi che fornisce una visione completa dei server PowerEdge, dello storage interno e di altri componenti. Include il rilevamento delle deviazioni per trovare modifiche rispetto a un template di configurazione definito dall'utente, crea avvisi e registri per tenere traccia dello stato del sistema e consente di correggere le configurazioni errate in base a policy preconfigurate. OpenManage include rollback del firmware, aggiornamenti centralizzati, rinnovo automatico dei certificati SSL (Secure Socket Layer) e deployment automatizzati per una configurazione di sicurezza coerente.

Risorse

Breve presentazione OpenManage Secure Enterprise Key Manager

Modelli base Understanding Confidential Computing with Trusted Execution Environments and Trusted Computing

Infografica Zero-trust architecture

Video Zero Trust

Quinta parte: favorire il successo dell'azienda con Dell Technologies e Intel

L'aumento della sofisticatezza e l'espansione della superficie di attacco delle minacce richiedono un approccio moderno alla cyber-resilienza. La nostra risposta consiste nell'aiutare a creare un'architettura Zero Trust con una gamma di strumenti e tecnologie. Il nostro approccio alla sicurezza consente controlli più granulari a partire dall'accesso e dall'autorizzazione e dall'estensione alla resilienza dei dati e del sistema, garantendo al contempo un'esperienza utente di livello superiore.

Con Dell Technologies e Intel come partner, si ottiene:

- Cyber-resilienza comprovata con sicurezza integrata, non aggiunta in un secondo momento
- Semplicità nel bilanciamento degli obiettivi aziendali e della produttività con sicurezza e privacy
- Una suite di hardware e software progettata per proteggere l'infrastruttura IT e offrire sicurezza, controllo e scalabilità per il profilo di sicurezza
- Vigilanza costante per mantenere un profilo di sicurezza robusto utilizzando una risposta rapida alle vulnerabilità e agli xploit comuni

Risorse

Pagina web Security solutions

Servizi di resilienza del business

Managed Detection and Response

Ulteriori informazioni sui server PowerEdge cyber-resilienti sono disponibili sul sito web Dell.com/Servers.

È possibile iscriversi al nostro popolare Power2Protect podcast di Dell Technologies e scoprire gli ultimi episodi sulla sicurezza e la cyber-resilienza.