Gateway con connessione sicura

La nostra tecnologia integra la protezione dei dati e la prevenzione delle minacce in un'esperienza di supporto sicura e automatizzata

Fino all'

60%

dei leader IT esaminati dalla tecnologia di connettività di per utilizzo ottimale Forrester per ridurre il rischio[1]

Viene anche implementata nella versione con connessione diretta per determinati hardware Dell EMC e come plug-in per i servizi di OpenManage Enterprise per i server PowerEdge. Dell Technologies Services si impegna al massimo per implementare le funzionalità di sicurezza nei nostri prodotti, in base ai mercati, alle normative e alle indicazioni dei clienti, consentendo di soddisfare i requisiti di conformità e gli obiettivi di sicurezza dei nostri clienti.

Sommario

1: Introduzione 3

2: Informazioni sul gateway con connessione sicura 4

3: Panoramica dell'architettura di sicurezza 5

4: Approccio dettagliato alla sicurezza per il gateway con connessione sicura 6

4-1: Data collection on-site sicura 6

Il gateway con connessione sicura funge da strumento sicuro per la gestione delle comunicazioni, consente ai clienti di controllare i requisiti di autorizzazione, utilizza i protocolli di autenticazione a due fattori e offre altre utili funzionalità.

4-2: Strumento sicuro di trasporto e comunicazione dei dati 9

Il gateway con connessione sicura utilizza la crittografia e l'autenticazione bilaterale per creare un tunnel TLS sicuro per heartbeat polling, notifica remota e funzioni di accesso remoto.

4-3: Processi sicuri di storage, utilizzo ed elaborazione dei dati 11

Ulteriori informazioni sulle numerose misure implementate quotidianamente per proteggere i dati tra cui sicurezza fisica, risk management della supply chain e processi di sviluppo sicuri.

5: Conclusioni 15

1: Introduzione:

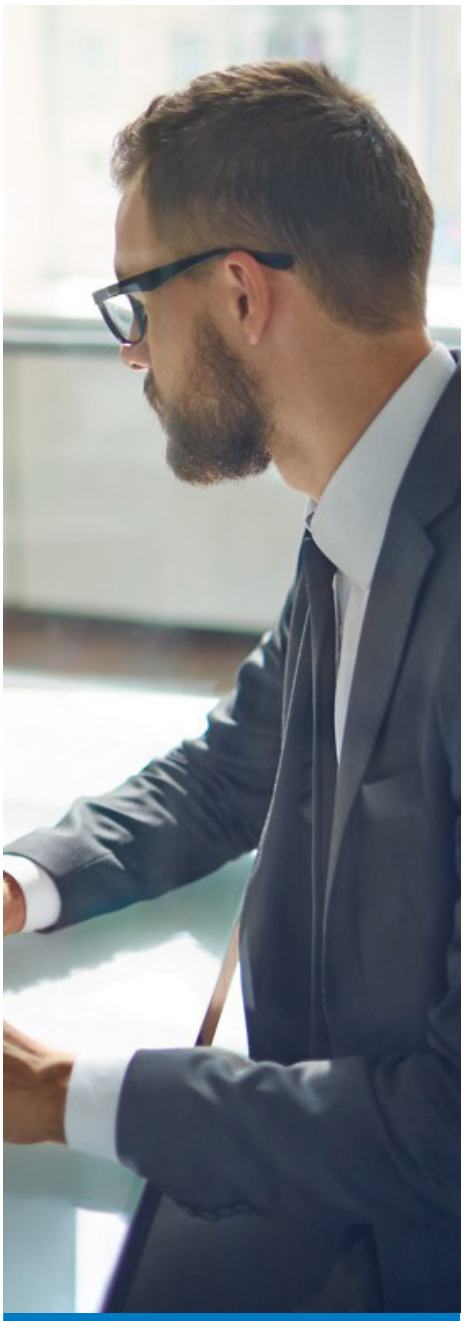
Nell'attuale era iperdigitale, i leader indiscussi dell'innovazione si avvalgono dell'outsourcing del supporto IT, affidandosi a fornitori di servizi IT. Secondo uno studio di Forrester Consulting commissionato da Dell Technologies Services[1], il 59% dei leader IT ritiene che una partnership con il giusto fornitore di servizi IT consenta loro di dedicare il tempo previsto per le operazioni quotidiane all'innovazione e a iniziative strategiche.

In qualità di fornitore di servizi IT leader del settore, Dell Technologies Services si impegna al massimo per assicurare che le tecnologie e i servizi di supporto IT offerti non siano potenziali fonti di minacce alla sicurezza. Ogni singolo giorno, facciamo tutto il possibile per ridurre al minimo i rischi derivanti dai prodotti Dell EMC implementati negli ambienti dei nostri clienti. Questo studio esamina in che modo la sicurezza è integrata nella progettazione, nell'implementazione e nelle operazioni del gateway con connessione sicura al fine di garantire un'esperienza di supporto IT automatizzata sicura per le infrastrutture di data center complesse.

Basato su oltre 25 anni di esperienza nella tecnologia all'avanguardia per il supporto IT, il gateway con connessione sicura è progettato per scongiurare qualsiasi violazione della sicurezza e proteggere l'integrità dei dati. La nostra tecnologia monitora costantemente i dispositivi dei clienti per rilevare eventuali problemi e avviarne la risoluzione rapida, assicurando allo stesso tempo:

- L'utilizzo solo dei dati di telemetria ed eventi dei sistemi attivi.
- La crittografia dei dati sullo stato del sistema per il trasporto tramite Internet su HTTPS utilizzando il protocollo TLS (Transport Layer Security).
- L'utilizzo dell'autenticazione a più fattori per l'accesso da remoto dei nostri ingegneri autorizzati del supporto tecnico per la risoluzione dei problemi dei sistemi connessi.
- L'adozione di procedure di sicurezza leader del settore per l'elaborazione, lo storage e l'utilizzo dei dati di telemetria ed eventi presso le nostre sedi.

Inoltre, verifichiamo scrupolosamente le misure di sicurezza integrate attraverso l'architettura e i processi del gateway con connessione sicura con i principali vendor, come Secureworks, per garantire ai clienti un'esperienza sempre sicura e riservata.



Gli attacchi informatici e le frodi e i furti di dati sono tra le dieci principali preoccupazioni dei CEO[2]

2: Informazioni sul gateway con connessione sicura

Dell Technologies offre una tecnologia di connettività sicura che semplifica la prevenzione dei problemi, consentendo ai clienti di dedicare più tempo ai progetti strategici. Le versioni dell'applicazione e dell'appliance virtuale forniscono una connessione bidirezionale sicura tra l'ambiente del cliente e Dell Technologies Services, ideale per monitorare i dispositivi Dell EMC di un data center, inclusi storage dei dati, server, reti, infrastrutture CI/HCI e sistemi di protezione dei dati, da un'unica console.

È anche possibile implementare in modo flessibile la nostra tecnologia nella versione con connessione diretta per determinati prodotti Dell EMC e come plug-in per i servizi di OpenManage Enterprise per i server PowerEdge. Visitare Dell.com/Support per verificare le opzioni di connettività supportate per hardware e software Dell EMC specifici.

I dati sono la linfa vitale del gateway con connessione sicura. Utilizziamo i dati sullo stato del sistema raccolti dagli ambienti dei clienti e li mettiamo in correlazione con dati su incidenti e progettazione acquisiti nel corso degli anni dai team del supporto tecnico e dai team sul campo, nonché dai produttori dei componenti.

Visualizzare i documenti sugli elementi inclusi nel report per il gateway con connessione sicura e il plug-in per i servizi di OpenManage Enterprise per i dettagli delle informazioni sullo stato del sistema raccolte.

Utilizzando sofisticati modelli di intelligenza artificiale (incluso l'apprendimento automatico), la nostra tecnologia di connettività è in grado di trovare e applicare pattern per individuare immediatamente l'esatto problema da risolvere, sia hardware sia software. Quindi, crea un caso e avvia i contatti per la risoluzione prima che diventi un problema costoso. Grazie alla connessione con il gateway con connessione sicura, prevede i guasti dei dischi rigidi e dei backplane dei server. A seconda del tipo di problema, l'avviso può avviare anche la spedizione automatica dei componenti.

Inoltre, la tecnologia abilita la comunicazione bidirezionale sicura per gli agenti autorizzati del supporto tecnico che possono accedere da remoto ai dispositivi gestiti per risolvere i problemi.

SICUREZZA PER LA CONNETTIVITÀ

Valutazioni della sicurezza di terze parti vengono condotte periodicamente per il gateway con connessione sicura e per la relativa infrastruttura di supporto.

Le valutazioni dell'applicazione includono: sicurezza del trasporto dei dati e dell'API, analisi del codice sorgente statico e dinamico, controlli incrociati CVE (Common Vulnerabilities and Exposures) e OWASP (Open Web Application Security Project), oltre a librerie e prodotti di terze parti.

Le valutazioni dell'infrastruttura includono: dispositivi di rete interni ed esterni, server e fornitori di servizi.

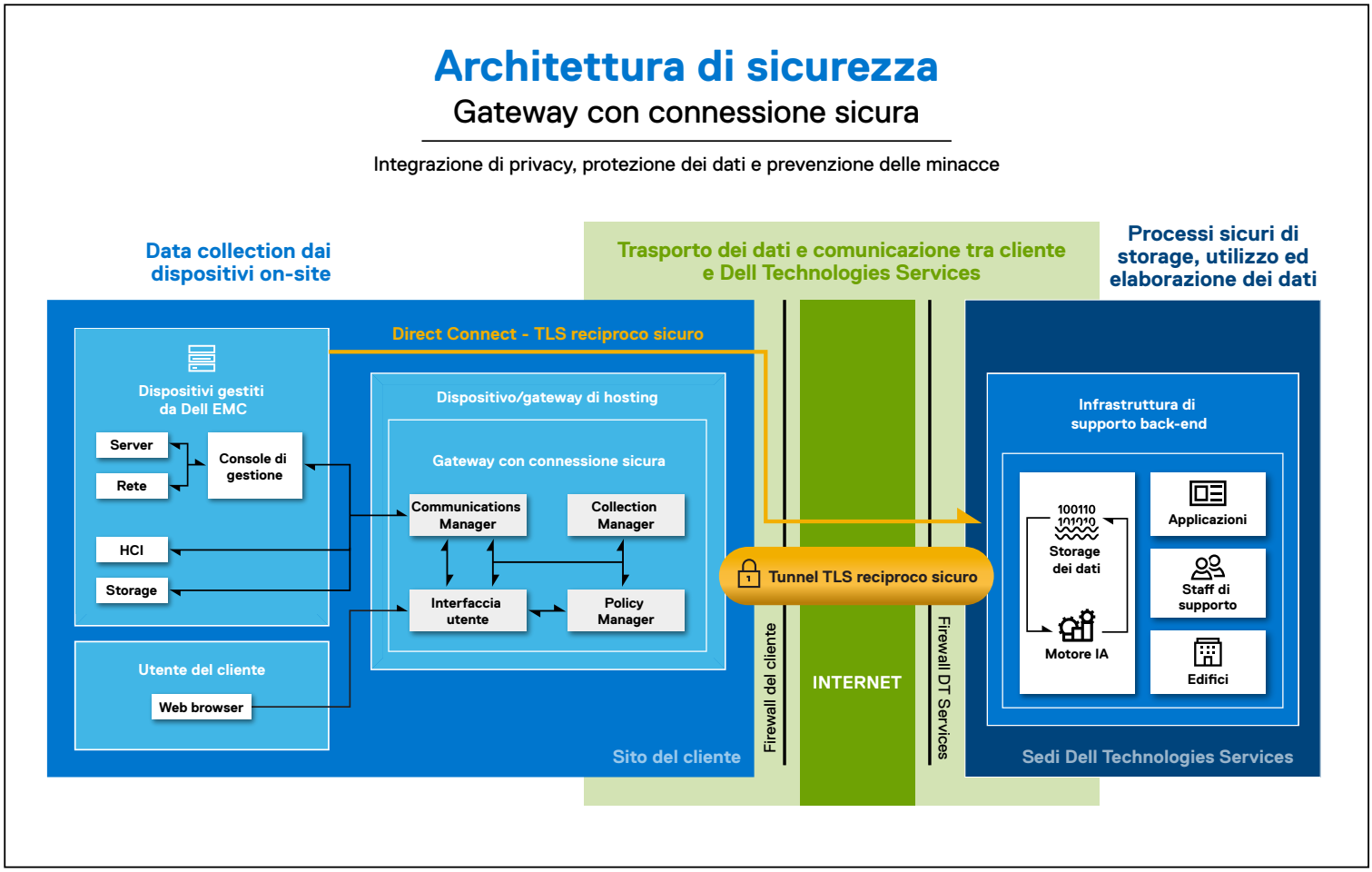
3: Panoramica dell'architettura di sicurezza

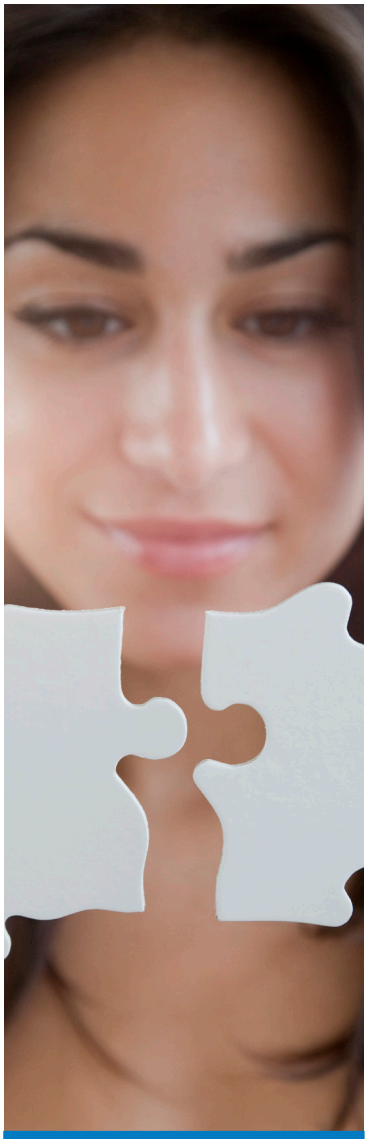
Dell Technologies Services si impegna a ridurre al minimo le minacce alla sicurezza correlate alla nostra tecnologia di connettività automatizzata, proattiva e predittiva. L'architettura di sicurezza è basata su rigorosi standard di settore e segue procedure di sicurezza misurabili e ripetibili in ogni fase di sviluppo e deployment dei prodotti. Per ulteriori informazioni, consultare la sezione 4.

Il diagramma A riportato di seguito fornisce una panoramica dell'architettura di sicurezza del gateway con connessione sicura. Nelle sezioni seguenti, analizzeremo dettagliatamente in che modo la nostra tecnologia raccoglie dai dispositivi gestiti da Dell EMC solo i dati sul sistema necessari per individuare e risolvere i problemi, quindi vedremo come tali dati vengono gestiti con la massima sicurezza, nel pieno rispetto della privacy:

- Data collection dai dispositivi on-site
- Trasporto e comunicazione dei dati
- Storage, utilizzo ed elaborazione dei dati presso le sedi Dell Technologies Services

Diagramma A:





I clienti ottengono un livello aggiuntivo di sicurezza per la data collection on-site grazie alle funzionalità di audit di Policy Manager incluse nel gateway con connessione sicura

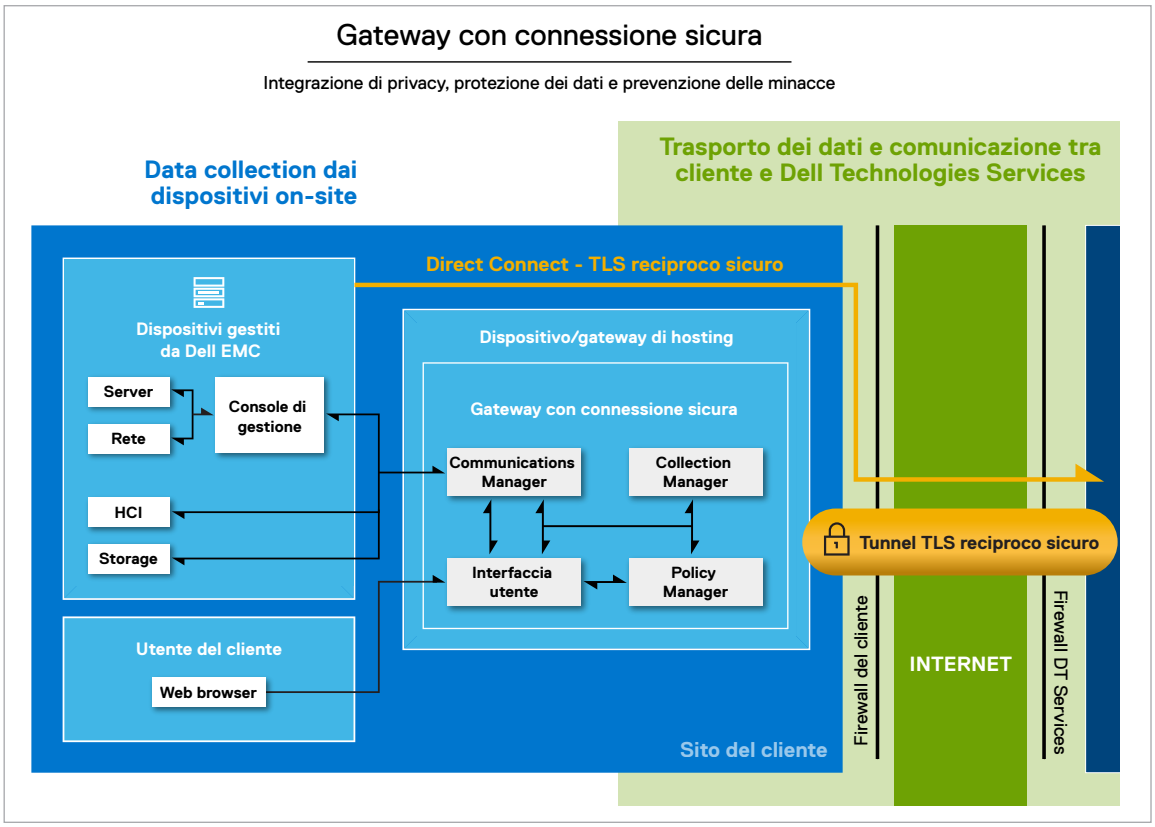
4: Approccio dettagliato alla sicurezza per il gateway con connessione sicura

4-1: Data collection on-site sicura

Riduzione al minimo dei punti di accesso del firewall

Il gateway con connessione sicura aggrega le comunicazioni dei dispositivi Dell EMC e funge da unico punto di ingresso e uscita nel firewall del cliente per l'attività di tutti i servizi remoti basati su IP (vedere il diagramma B). Riducendo al minimo i punti di accesso del firewall per la tecnologia di supporto IT da remoto, Dell Technologies limita il rischio per la sicurezza correlato al firewall dell'azienda.

Diagramma B: (estratto dal diagramma A - Architettura di sicurezza):



Come gateway on-site, il gateway con connessione sicura viene implementato virtualmente su un hypervisor fornito dal cliente. Ogni server gateway funge da proxy, trasportando informazioni sui/dai dispositivi gestiti. Inoltre, il gateway con connessione sicura può creare una coda degli eventi Connect Home in caso di problemi temporanei della rete locale. Questi server gateway sono dotati di una propria interfaccia utente web basata sul sistema operativo sottostante.

La versione con connessione diretta è adatta ai deployment eterogenei con più prodotti hardware Dell EMC. Questa soluzione fornisce un singolo punto sicuro per le comunicazioni attraverso il firewall del cliente. È integrata nell'ambiente operativo del prodotto, pertanto non richiede un server separato per il supporto remoto in entrata e per la funzionalità Call Home.

Riduzione al minimo dei punti di accesso del firewall (continua)

Nei data center PowerEdge che utilizzano la console di system management OpenManage Enterprise, il plug-in per i servizi integrato è un'opzione di implementazione alternativa. Questo plug-in per la connettività nell'appliance virtuale OpenManage Enterprise viene eseguito su un hypervisor fornito dal cliente. Funge da livello di automazione dei servizi dei dispositivi gestiti su server e chassis e fornisce una connessione diretta singola e sicura al back-end di Dell Technologies Services.

Strumento sicuro per la gestione delle comunicazioni

Il gateway con connessione sicura funge da strumento per la gestione delle comunicazioni tra i dispositivi gestiti, Policy Manager e l'infrastruttura di supporto back-end di Dell Technologies Services. I server gateway su cui è implementato sono gestori HTTPS. Il gateway utilizza diversi metodi di comunicazione per l'individuazione dei dispositivi, la gestione degli eventi e la data collection e la gestione dei dati di telemetria. I tipi di messaggi includono:

- Heartbeat polling dello stato dei dispositivi
- Trasferimento dei file di dati (Connect Home)
- Trasferimento dei dati di utilizzo delle licenze
- Richieste di autenticazione utente
- Sincronizzazione della gestione dei dispositivi

Tutti i messaggi vengono protetti grazie a molteplici protocolli. In una delle sezioni seguenti esamineremo più dettagliatamente il livello aggiuntivo di sicurezza integrato nel trasporto e nella comunicazione dei dati del gateway con connessione sicura, incluso l'utilizzo del protocollo HTTPS con tunneling TLS (Transport Layer Security) end-to-end e crittografia standard del settore.

Controllo dei requisiti di autorizzazione e delle autorizzazioni di accesso per il cliente

Se i dispositivi sono monitorati dal gateway con connessione sicura nel data center del cliente, è possibile scegliere di utilizzare Policy Manager per controllare i requisiti di autorizzazione per le connessioni di accesso remoto, l'esecuzione di script di diagnostica e altre attività correlate. I clienti possono impostare autorizzazioni di accesso non solo per il personale, ma anche per gli ingegneri del supporto tecnico che si connettono da remoto per diagnosticare e risolvere i problemi.

La sicurezza della gestione delle autorizzazioni è garantita dalle seguenti funzioni di Policy Manager:

- Il gateway con connessione sicura esegue periodicamente il polling di Policy Manager per rilevare eventuali modifiche delle autorizzazioni, quindi memorizza le autorizzazioni nella cache locale. Policy Manager consente le seguenti impostazioni:
  - La cache del set di regole viene aggiornata automaticamente con gli aggiornamenti della configurazione dopo l'ultimo ciclo di polling.
  - La configurazione per ricevere messaggi come listener HTTPS su una specifica porta concordata.
- Quando il gateway con connessione sicura riceve una richiesta di accesso remoto o di esecuzione di altre azioni, applica la policy ricevuta dalla cache di Policy Manager.
  - Le autorizzazioni possono essere assegnate in ordine gerarchico con policy basate sul tipo di dispositivo o su modelli specifici di un tipo di dispositivo.
  - I clienti possono accettare o rifiutare l'azione richiesta tramite l'interfaccia utente web di Policy Manager. Inoltre, possono creare filtri per limitare ulteriormente le autorizzazioni e le azioni.

Registrazione e audit trail

Ai clienti viene assicurato un livello aggiuntivo di sicurezza per la data collection on-site tramite le funzionalità di audit di Policy Manager nel gateway con connessione sicura. Policy Manager registra tutti gli eventi, le connessioni, le esecuzioni degli script di diagnostica e le operazioni di trasferimento dei file di supporto dei servizi remoti. Quindi, li memorizza nel proprio database come semplici file di testo di audit log. Inoltre, monitora l'accesso a Policy Manager, le modifiche delle policy e tutti gli accessi, sia autorizzati sia negati.

I clienti hanno tutte queste informazioni a portata di mano poiché:

- Gli audit vengono visualizzati tramite l'interfaccia utente web di Policy Manager e non possono essere modificati.
- Gli audit log possono essere configurati in modo da essere trasmessi al server syslog del proprio ambiente.

Gateway con connessione sicura

Suite di crittografia TLS 1.2 supportate:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Opzione di sicurezza per il controllo dei dispositivi

Poiché i clienti non sempre attivano Policy Manager per la gestione delle autorizzazioni, il gateway con connessione sicura fornisce delle funzionalità di protezione tramite l'opzione di controllo dei dispositivi.

I clienti possono:

- Creare gruppi personalizzati basati su tipo di dispositivo, amministratore del gruppo, organizzazione o business unit, posizione fisica del dispositivo o qualsiasi altro criterio desiderato
- Definire autorizzazioni e diritti di accesso specifici per i device group

Vengono registrate tutte le operazioni di gestione dei dispositivi, inclusa l'attività remota eseguita dagli ingegneri del supporto tecnico. Esse devono essere approvate nel back-end da un agente del supporto tecnico.

In questo modo, i clienti mantengono il pieno controllo e la visibilità dei dispositivi gestiti tramite il gateway con connessione sicura.

Autenticazione a due fattori e gestione dei certificati digitali

L'autenticazione è un componente importante della data collection on-site sicura. Il gateway con connessione sicura utilizza un certificato digitale come prova di identità del proprio deployment sul server gateway del cliente. Il certificato associa l'identità del server gateway alla coppia di chiavi per la crittografia e l'autenticazione della comunicazione nel back-end. L'Autorità di certificazione (CA) di Dell Technologies Services è il repository centrale per l'infrastruttura delle chiavi del gateway con connessione sicura.

La gestione dei certificati digitali viene utilizzata per automatizzare l'iscrizione del certificato digitale tramite la nostra Autorità di certificazione. Ciò:

- Abilita la generazione e l'autenticazione programmatiche di ogni richiesta di certificato.
- Garantisce che il certificato venga emesso e installato esclusivamente sul server gateway. Il certificato non può essere copiato o usato su un altro sistema.

Il gateway con connessione sicura esegue la connessione e l'autenticazione utilizzando il certificato digitale implementato sulla nostra infrastruttura del supporto back-end. Gli agenti del supporto tecnico si collegano al gateway con connessione sicura nell'ambiente del cliente utilizzando l'autenticazione a due fattori.

4-2: Strumento sicuro di trasporto e comunicazione dei dati

Tunnel di comunicazione sicuro

Tutte le comunicazioni in uscita tra il cliente e l'infrastruttura del supporto back-end di Dell Technologies Services vengono avviate dal gateway con connessione sicura dalla sede del cliente. Viene creato un tunnel di comunicazione end-to-end sicuro che utilizza la crittografia a 256 bit TLS (Transport Layer Security) standard del settore su Internet e l'autenticazione con certificato digitale firmato da Dell Technologies Services. Quest'ultimo processo viene descritto nella sezione precedente dedicata alla data collection on-site sicura.

Pertanto, le connessioni del gateway con connessione sicura vantano le seguenti caratteristiche:

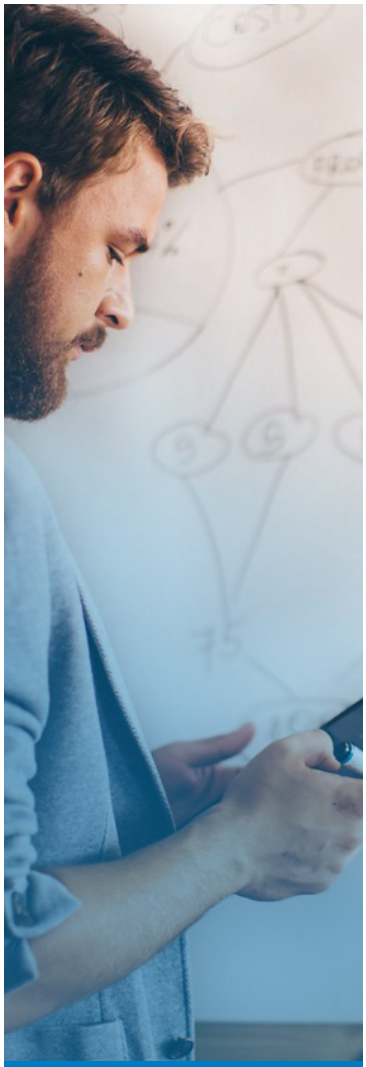
- **Trasferimento affidabile dei dati:** ogni messaggio trasmesso include un controllo di integrità che utilizza un codice di autenticazione del messaggio per impedire il mancato rilevamento di perdite o modifiche dei dati durante la trasmissione.
- **Sessione privata e sicura tramite TLS:** la crittografia simmetrica con algoritmi standard del settore genera chiavi univoche per ogni connessione. Qualsiasi modifica delle comunicazioni durante la navigazione viene rilevata.
- **Parti autenticate:** poiché è sicura, questa connessione identifica le parti che comunicano e le autentica utilizzando la crittografia a chiave pubblica. Questo approccio impedisce gli attacchi di tipo spoofing e MITM (Man-In-The-Middle).

Comunicazioni tramite tunnel TLS sicuro

Il server gateway utilizza il tunnel TLS per garantire un ambiente sicuro per le seguenti funzioni: heartbeat polling, notifica remota e accesso remoto. In questa sezione e nel diagramma C, esamineremo più dettagliatamente i principali processi e protocolli di comunicazione alla base dell'esperienza automatizzata, proattiva e predittiva offerta dalla nostra tecnologia.

Heartbeat polling

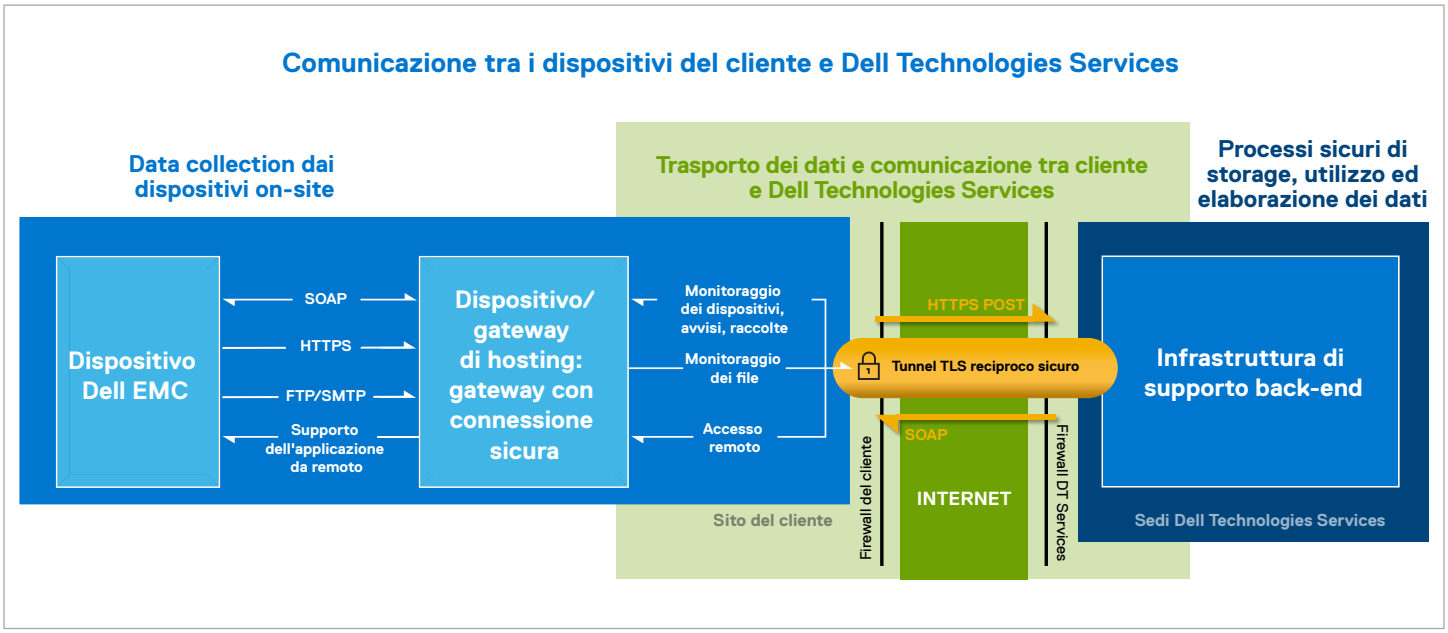
Per utilizzare il gateway con connessione sicura, i sistemi dei clienti devono essere connessi. Heartbeat polling verifica lo stato di connessione dei dispositivi e comunica periodicamente i dati di telemetria raccolti al back-end. I dati identificano anche il server gateway su cui il gateway con connessione sicura è implementato.



L'autenticazione leader del settore protegge le connessione dagli attacchi di tipo spoofing e MITM (Man-In-The-Middle)

Comunicazioni tramite tunnel TLS sicuro (continua)

Diagramma C: Architettura di sicurezza



Notifica remota o funzione Connect Home

Il gateway con connessione sicura funge da canale sicuro per l'invio dei file di evento dai dispositivi al back-end, come errori, avvisi, condizioni di avvertenza, report sullo stato, dati di configurazione e stati di esecuzione degli script.

- Quando viene generato un avviso, viene creato un file di evento che viene inviato al gateway.
- Il file viene ricevuto dal gateway con connessione sicura tramite i servizi listener HTTPS.
- Per i prodotti legacy che utilizzano listener FTP e/o SMTP per il gateway con connessione sicura, i file vengono crittografati e trasferiti.
- Il gateway comprime il file e lo invia al back-end tramite il tunnel TLS, quindi lo elimina dalla directory del listener.
- Il file viene decompresso nel back-end per l'analisi.
- Il gateway con connessione sicura può inviare i file al back-end anche tramite il tunnel di comunicazione crittografato. Inoltre, il gateway può essere configurato in modo da utilizzare i canali di failover, ovvero il server FTPS o e-mail del cliente.

I dati di monitoraggio del sistema vengono raccolti dai vari componenti di un sistema attivo per consentire a Dell Technologies Services di fornire un'esperienza di supporto adattiva, intelligente e rapida. L'ID sistema, necessario per identificare il sistema specifico su cui si sta lavorando, è l'unica informazione raccolta dai dispositivi. Quando stabiliamo che un componente deve essere spedito in modo proattivo, utilizziamo le informazioni di contatto memorizzate in modo sicuro sui server Dell Technologies.

Un elenco completo dei dati di monitoraggio del sistema raccolti da un sistema attivo, inclusi i dati raccolti al di fuori del ciclo normale di 24 ore, è disponibile nei documenti sugli elementi inclusi nel report per il gateway con connessione sicura e il plug-in per i servizi di OpenManage Enterprise.

Accesso remoto

Anche i nostri team del supporto tecnico accedono da remoto ai dispositivi presso il sito del cliente per risolvere i problemi o eseguire azioni specifiche su un dispositivo. La messaggistica asincrona garantisce che la sessione di accesso remoto venga avviata dal gateway con connessione sicura dal sito del cliente. Successivamente, una sessione di accesso remoto sicura viene stabilita nel modo seguente:

- Dopo l'autenticazione della sessione nel back-end di Dell Technologies Services, un agente del supporto tecnico richiede l'accesso al dispositivo, includendo il numero di Service Request, se disponibile, e altre informazioni di identificazione del dispositivo o dell'utente.
- La richiesta di accesso remoto viene inserita nella coda del back-end finché il gateway non invia il messaggio heartbeat del dispositivo al back-end per recuperarla.
- In risposta, il server back-end invia una risposta che include le informazioni sulla richiesta, l'indirizzo del server back-end e l'ID sessione univoco per la connessione al gateway.
- Il gateway con connessione sicura utilizza il proprio repository locale per determinare l'indirizzo IP locale del dispositivo. Quindi, controlla la policy memorizzata nella cache da Policy Manager per verificare le autorizzazioni di connessione.
- Se consentito, il gateway con connessione sicura stabilisce una connessione TLS persistente separata al server back-end. La connessione TLS viene sempre avviata dal gateway. Il server back-end non può mai avviare una connessione in entrata al server gateway. Ciò garantisce che non vi sia alcuna vulnerabilità agli attacchi esterni.

La comunicazione avviene attraverso il tunnel tra il gateway con connessione sicura e il server back-end finché non viene terminata o non scade dopo un periodo di inattività.

Sicurezza della rete

Tutti i componenti di monitoraggio della rete sono protetti da firewall e sono gestiti dal nostro team responsabile della sicurezza di rete. Il traffico di rete viene rigorosamente controllato. Tutto il traffico in entrata viene trasmesso tramite porte specifiche e viene inviato agli indirizzi di rete di destinazione appropriati.

4-3: Processi sicuri di storage, utilizzo ed elaborazione dei dati

Sicurezza per storage e utilizzo

Sicurezza fisica

Dell Technologies Services ospita la maggior parte dei dati del gateway con connessione sicura (come le informazioni su applicazioni, sistemi, componenti di rete e sicurezza) in un data center negli Stati Uniti, progettato per assicurare alti livelli di disponibilità e sicurezza. I dati sono protetti da numerose misure, inclusi strumenti di sicurezza fisica. Ecco solo alcune delle misure adottate:

- Addetti alla sicurezza on-premise
- Fotocamere
- Falsi ingressi
- Barriere per veicoli
- Progettazione specifica dei parcheggi
- Muri e vetri anti-proiettili
- Utilizzo di edifici anonimi

L'accesso all'infrastruttura dove risiedono i data center è consentito esclusivamente al personale autorizzato. L'accesso è controllato tramite smart card.

Sicurezza logica

I dati generati dal gateway con connessione sicura sono memorizzati in conformità all'Informativa sulla privacy Dell.

L'accesso logico all'infrastruttura Dell Technologies Services (server, sistemi di bilanciamento del carico, share di rete, ecc.) è consentito esclusivamente tramite strumenti interni che sono controllati e valutati in conformità alle linee guida IT:

Sicurezza logica (continua)

- **Sicurezza di server e database:** i componenti dei server e dei sistemi operativi risiedono su immagini standard che sono state sottoposte a controlli di sicurezza. Gli aggiornamenti della sicurezza, inclusi quelli pubblicati da Microsoft e da altri vendor di software, vengono verificati periodicamente. Quando vengono rilasciati importanti aggiornamenti della sicurezza, essi vengono prima testati su immagini non di produzione e poi applicati tempestivamente ai server attivi per evitare qualsiasi rischio.
- **Verifica:** i log dei dispositivi monitorati vengono conservati e sono accessibili esclusivamente da infrastrutture e applicazioni Dell Technologies Services autorizzate. Questi log registrano tutti i tentativi di connessione o accesso al sistema operativo o alla console del server web del gateway con connessione sicura.

La protezione delle build gestite dall'IT è rafforzata attraverso l'uso delle best practice di sicurezza dei controlli del CIS (Center for Internet Security). Inoltre, vengono implementate le linee guida di sicurezza standard del settore su tutti i server e su tutte le apparecchiature di rete.

Infine, l'ecosistema del gateway con connessione sicura sfrutta sia l'high availability locale del proprio data center sia un'infrastruttura identica in un data center separato. Le uniche eccezioni sono le tecnologie con high availability intrinseca, come cluster Big Data e private cloud. Per l'analisi dei dati, Dell Technologies Services utilizza ambienti cloud che controlliamo e gestiamo completamente, inclusi private cloud, hybrid cloud e public cloud.

Autenticazione

Il gateway con connessione sicura utilizza Dell MyAccount per l'autenticazione con Dell Technologies Services e i gruppi di accesso OS per l'autenticazione on-the-box.

Ai gruppi, come il team di amministrazione database e il team di supporto operativo, che dispongono dell'accesso ai componenti del gateway con connessione sicura, vengono assegnati compiti e diritti di accesso separati. Tutti gli aggiornamenti apportati all'ambiente di produzione vengono sottoposti a una procedura di controllo delle modifiche definita che integra controlli e bilanciamenti.

Utilizziamo un processo di sviluppo ripetibile e sicuro per i prodotti e le applicazioni

Sicurezza dei processi

Community attenta alla sicurezza

Offriamo un programma di formazione per la sicurezza basato su ruoli multi-livello per istruire i dipendenti nuovi ed esistenti sulle best practice per la sicurezza specifiche di job e su come utilizzare le risorse rilevanti. Dell Technologies si impegna al massimo per creare una cultura consapevole della sicurezza nell'intera community. Inoltre, la nostra community di sviluppatori fa parte del programma Security Champion di Dell, che è stato progettato per favorire la sicurezza shift-left nelle procedure di sviluppo del software.

Sviluppo

Il nostro **standard SDL (Secure Development Lifecycle)** interno è un riferimento comune per le organizzazioni dei prodotti Dell Technologies per valutare la sicurezza delle attività di sviluppo delle applicazioni e dei prodotti e confrontarla con le aspettative del mercato e le procedure del settore. Questo standard definisce i controlli di sicurezza che i team dei prodotti devono adottare quando sviluppano nuove funzioni e funzionalità. Lo standard SDL include sia attività di analisi sia controlli proattivi prescrittivi per le principali aree di rischio. Le attività di analisi, come modellazione delle minacce, analisi di codice statico, scansioni e test di sicurezza, hanno l'obiettivo di individuare e risolvere difetti correlati alla sicurezza in tutto il ciclo di sviluppo. I controlli prescrittivi, invece, hanno l'obiettivo di garantire che i team di sviluppo creino codice in modo sicuro per impedire problemi specifici di sicurezza come le "Dieci Vulnerabilità più Critiche delle Applicazioni Web" di OWASP (Open Web Application Security Project) o gli errori evidenziati dalle relazioni di SANS (Top 25). Il gateway con connessione sicura ha adottato

Sviluppo (continua)

Dell SDL Maturity Framework per l'implementazione dei controlli di sicurezza in linea con gli standard del settore.

Il codice del gateway con connessione sicura è stato sviluppato utilizzando la metodologia di sviluppo Agile. Il codice viene integrato continuamente utilizzando un software di automazione standard del settore. Le versioni del codice vengono archiviate e controllate utilizzando le autorizzazioni del gruppo di sicurezza.

Ogni versione software viene sottoposta a una valutazione della sicurezza in conformità alle nostre policy di sicurezza che includono:

- Valutazione delle vulnerabilità con test di penetrazione
- Test di sicurezza di terze parti con l'utilizzo delle tecnologie di vendor leader del settore come Secureworks
- Valutazione per le soluzioni di gestione dell'autenticazione, dell'autorizzazione e delle identità
- Tutte le librerie e i componenti di terze parti vengono esaminati con soluzioni leader del settore per l'analisi della composizione del software. Inoltre, i consulenti Dell Security vengono informati dei miglioramenti di sicurezza specifici.
- Classificazione dei dati con la nostra organizzazione Global Security. Questo processo integra privacy e sicurezza per garantire la protezione dei dati elettronici.

Le applicazioni sono sottoposte anche a governance e audit di sicurezza.

Gestione delle modifiche

Il processo di gestione delle modifiche di Dell Technologies segue le best practice ITIL Foundation come richiesto dal nostro comitato aziendale per il controllo delle modifiche. Tutte le modifiche sono gestite tramite ticket di richiesta di modifica. Gli utenti che accedono al nostro sistema per apportare modifiche devono prima seguire la formazione ITIL, oltre ad acquisire familiarità con il linguaggio SDL. Tutti gli aggiornamenti e gli upgrade applicati all'infrastruttura back-end sono sottoposti a un processo di controllo delle versioni per garantirne il monitoraggio e la tracciabilità. Il team impiega un processo di compilazione automatizzato per applicare o revocare nuove build o hotfix implementate.

L'applicazione installata presso la sede del cliente può essere aggiornata in base alle preferenze del cliente. Ogni versione promossa sul sito Dell.com/support contiene informazioni sulle modifiche introdotte e le eventuali limitazioni note.

Tutte le nuove funzioni e modifiche vengono curate dal nostro team di gestione prodotti e sono organizzate secondo priorità in base a un processo di cambiamento pianificato che deve essere rivisto e approvato dal comitato per il controllo delle modifiche.

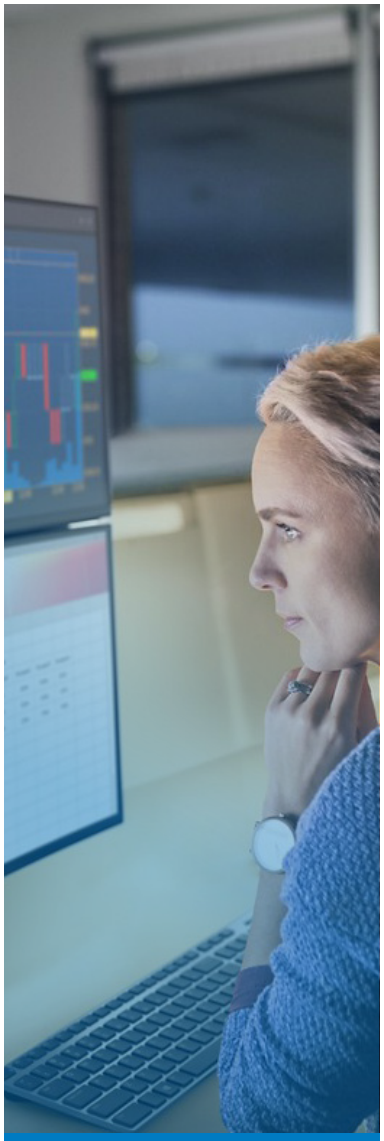
Risk management della supply chain

Dell Technologies segue le best practice leader del settore in ogni fase del ciclo di vita della supply chain (Plan, Source, Make, Deliver, Return). Adottiamo un approccio completo alla protezione della nostra supply chain che include anche la promozione di standard SCRM e best practice internazionali, al fine di confermare la nostra posizione di fornitore ICT affidabile nel marketplace globale.

Per saperne di più sulle procedure per la garanzia della supply chain cliccare qui.

Reporting sugli incidenti

Chiunque in Dell Technologies osservi attività sospette o sospetti un problema o una minaccia di cybersecurity deve segnalare immediatamente l'incidente al nostro team CSIRT (Computer Security Incident Response Team). Si può trattare di punti di debolezza o gap in un processo di sicurezza che potrebbero influire sul nostro ambiente o determinare una violazione dei sistemi e/o dei dati. Il CSIRT avvia quindi un'indagine completa sull'incidente e la persona che ha segnalato l'incidente fornisce tutti gli artefatti e i dettagli necessari affinché il CSIRT effettui l'indagine. Il team CSIRT utilizza il piano di risposta agli incidenti CSIRT, che descrive in dettaglio un processo formale per rispondere e risolvere incidenti di cybersecurity interni Dell e non del cliente. Questi incidenti possono rappresentare potenziali minacce per asset, reti di computer o apparecchiature per l'elaborazione dei dati Dell, nonché per Dell e le relative società controllate, personale, fornitore di servizi, partner o informazioni del cliente.



Collaborazione del settore sulle best practice per la sicurezza dei prodotti

Risposta alle vulnerabilità

Dell Technologies si impegna per ridurre al minimo i rischi associati alle vulnerabilità di sicurezza nei nostri prodotti fornendo ai clienti informazioni tempestive, indicazioni e strumenti di prevenzione per affrontare le minacce correlate alle vulnerabilità. Il nostro team PSIRT (Product Security Incident Response Team) è responsabile del coordinamento della risposta e della divulgazione di tutte le vulnerabilità dei prodotti che ci vengono segnalate. Tutte le divulgazioni sulla vulnerabilità dei prodotti Dell Technologies sono disponibili online.

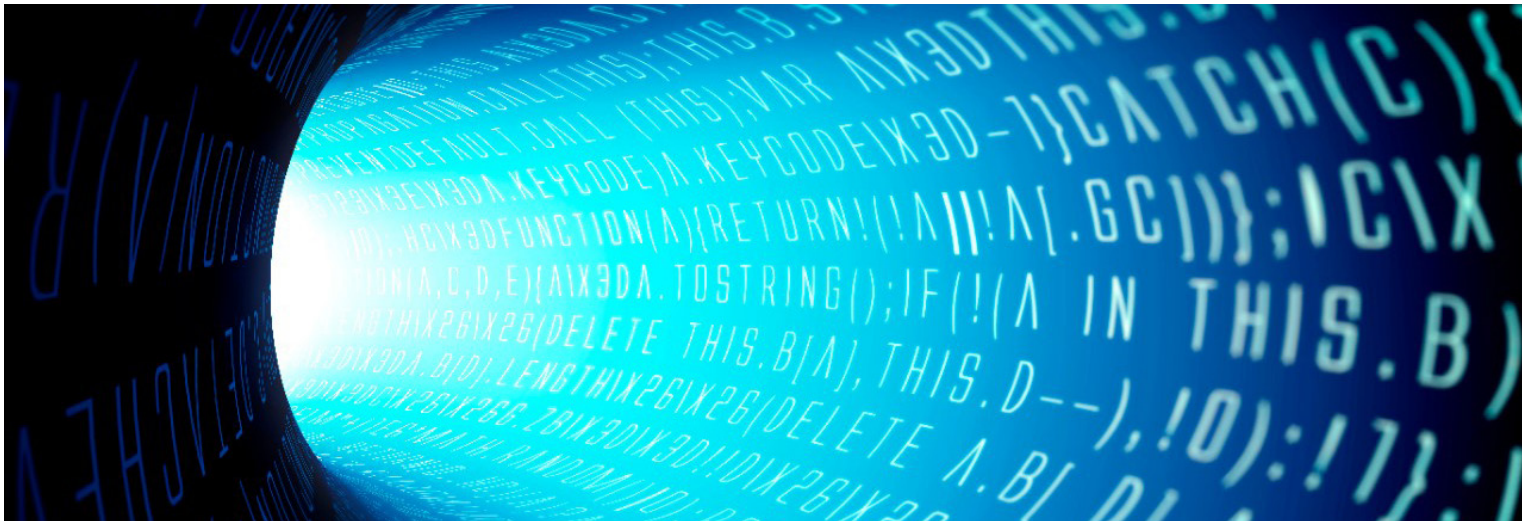
Ulteriori informazioni sulla nostra policy di risposta alle vulnerabilità

Affiliazioni di settore

Dell Technologies partecipa a diversi gruppi del settore per collaborare con gli altri principali vendor alla definizione, all'evoluzione e alla condivisione delle best practice per la sicurezza dei prodotti e promuovere le metodologie di sviluppo sicuro. Ecco alcuni esempi di collaborazione del settore:

- Dell, attraverso la sua entità EMC, ha co-fondato SAFECode (Software Assurance Forum for Excellence in Code) e attualmente ne presiede il Consiglio di Amministrazione. Altri membri del Consiglio includono rappresentanti di Microsoft, Adobe, SAP, Intel, Siemens, CA e Symantec. I membri di SAFECode condividono e pubblicano procedure e materiale di formazione per la sicurezza del software.
- Dell Technologies è un membro attivo del Forum for Incident Response and Security Teams (FIRST). FIRST è un'importante organizzazione riconosciuta come leader globale nella risposta agli incidenti e alle vulnerabilità.
- Partecipiamo attivamente all'Open Group Trusted Technology Forum (OTTF). OTTF guida lo sviluppo del programma e del framework per l'integrità della supply chain globale.
- Dell è stata una delle prime 9 aziende valutate nell'ambito del progetto Building Security In Maturity Model (BSIMM) nel 2008 e da allora ha continuato a partecipare al progetto. Un rappresentante di Dell Technologies fa parte del Comitato consultivo di BSIMM.
- I dipendenti Dell sono membri fondatori dell'IEEE Center for Secure Design, un progetto lanciato nell'ambito dell'iniziativa per la sicurezza informatica di IEEE per aiutare i Software Architect a comprendere e correggere i difetti di progettazioni correlati alla sicurezza.

Visitare il nostro Centro sicurezza e affidabilità per conoscere le risorse e le soluzioni che consentono di trovare risposte alle domande di sicurezza aziendale.



Standard di sicurezza del settore

I nostri dipendenti partecipano attivamente agli organismi di standardizzazione e ai consorzi del settore che si occupano di sviluppare standard di sicurezza e di definire procedure di sicurezza per tutto il settore, tra cui:

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- Forum for Incident Response and Security Teams (FIRST)
- International Committee for Information Technology Standards (INCITS)
- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- The Open Group
- Organization for the Advancement of Structured Information Standards (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

Certificazione ISO 9001

Dell Technologies vanta la certificazione ISO 9001. L'azienda conduce audit trimestrali e revisioni di conformità regolari per i propri centri di sviluppo e produzione.

5: Conclusioni

La nostra tecnologia di connettività offre un'esperienza di supporto IT semplificata con avvisi proattivi e predittivi automatizzati che garantiscono il massimo uptime per l'infrastruttura dei data center critici. Dell Technologies Services si impegna al massimo per offrire ai propri clienti un'esperienza estremamente sicura e riservata per la raccolta, la comunicazione, il trasporto, l'uso e lo storage dei dati di telemetria.

Per qualsiasi domanda o ulteriori informazioni, visitare l'indirizzo DellTechnologies.com/SecureConnectGateway

1 Fonte: "The Role Of IT Services Providers Expands To Strategic Collaboration", uno studio condotto da Forrester Consulting per conto di Dell Technologies, aprile 2021

2 Fonte: World Economic Forum Global Risks Report 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf