Panoramica di SupportAssist for Business PCs

Cinque domande chiave sulla sicurezza di SupportAssist e le loro risposte.

SupportAssist automatizza il supporto di Dell Technologies identificando i problemi hardware e software nell'intera flotta di PC. SupportAssist risolve i problemi relativi alla stabilizzazione e alle prestazioni del sistema, riduce le minacce alla sicurezza, monitora e rileva i guasti hardware e automatizza il processo di interazione con il supporto tecnico Dell.

SupportAssist, inoltre, raccoglie i dati di telemetria in modo proattivo dai PC e fornisce informazioni sull'utilizzo dei PC e sulle correzioni in base al piano di assistenza.

Sommario

I: Introduzione

Il guasto di un notebook può generare frustrazione, ma anche avere gravi conseguenze. Questi problemi possono avere un impatto significativo sulla produttività di un dipendente, spesso nel peggior momento possibile. Per questo motivo, i CIO delle aziende sono sempre più attenti alla qualità e all'uptime delle flotte di PC.

Molti CIO hanno adottato la tecnologia più recente e avanzata, che utilizza le informazioni acquisite dalla Data Science per elaborare miliardi di data point e migliorare l'efficienza degli amministratori IT. Le informazioni sullo stato del sistema provenienti dai sistemi degli utenti finali vengono inviate al reparto IT dell'azienda o a un fornitore di hardware o software per risolvere o prevenire rapidamente i problemi. Dell ProSupport Plus con tecnologia di connettività SupportAssist invia un avviso in caso di guasto del disco rigido, fornendo una vista centralizzata dell'intera flotta di PC dal portale TechDirect.

Sebbene questa tecnologia sia necessaria per garantire uptime ed efficienza, a volte i CIO hanno delle perplessità circa le informazioni raccolte e la loro gestione.

Le seguenti domande sono considerate critiche:

- Quali dati raccoglie SupportAssist?
- Come avviene la protezione dei dati raccolti nel momento in cui sono trasmessi al dipartimento IT dell'azienda o al fornitore del computer?
- Una volta arrivati a destinazione, archiviate i dati garantendo riservatezza e sicurezza?
- In che modo Dell rispetta il GDPR e altri standard?

Il documento esamina queste e altre domande correlate, al fine di valutare le tecnologie abilitate dalla Data Science. Offre una breve panoramica di come SupportAssist, parte di ProSupport Suite for PCs, fornisce un servizio di supporto completo in grado di prevedere e risolvere i problemi prima che si verifichino. Fornisce inoltre un'analisi più dettagliata sul modo in cui Dell Technologies Services protegge i dati sensibili nei processi, nel trasporto e nello storage dei dati.

II: Informazioni su SupportAssist

SupportAssist è la tecnologia di connettività intelligente[1] di Dell che consente alle organizzazioni di ricevere supporto tecnico automatizzato per l'intera flotta di PC. Monitora i dispositivi degli utenti finali, rileva in modo proattivo i problemi hardware e software e fornisce informazioni sull'uso del sistema.

Quando viene rilevato un problema, SupportAssist apre automaticamente una richiesta di assistenza con il supporto tecnico, in base al piano di assistenza. Il tipo di problema determinerà se l'avviso avvia una richiesta di supporto tecnico o attiva una spedizione automatica delle parti. SupportAssist raccoglie i dati hardware e software utilizzati dal supporto tecnico per risolvere il problema.

Dell ProSupport Suite for PCs offre le funzionalità di supporto più complete in un'unica soluzione, senza necessità di combinare i servizi.[2] Ulteriori informazioni.

Caratteristiche principali

- Rilevamento proattivo e predittivo a livello di flotta per accelerare la risoluzione dei problemi
- Analisi rapida dei punteggi relativi a salute, esperienza applicativa e sicurezza in un'unica schermata
- Una libreria di script creati da Dell per automatizzare le attività e risolvere i problemi in tutta la flotta
- Automatizzazione di creazione e deployment di cataloghi di aggiornamento personalizzati per BIOS, driver, firmware e applicazioni Dell
- Flessibilità nel personalizzare le visualizzazioni e i dashboard in TechDirect

Le funzioni disponibili variano in base al piano di supporto acquistato per un PC.

- Con ProSupport Plus, gli utenti finali ricevono la gamma completa delle funzioni di SupportAssist, tra cui il rilevamento predittivo dei problemi e la prevenzione dei guasti.

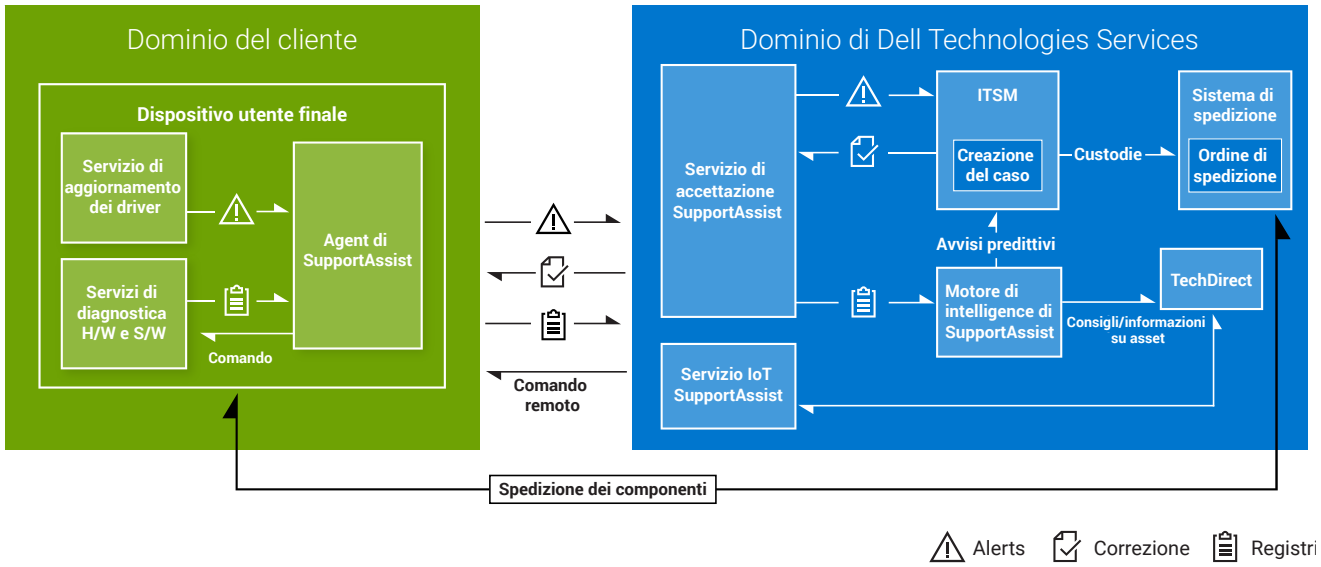
La Guida dell'amministratore contiene un elenco completo delle caratteristiche e delle funzionalità.

III. Architettura di SupportAssist

SupportAssist include una serie di servizi che monitorano costantemente i sistemi ed eseguono controlli integrità pianificati su un dispositivo. Queste informazioni vengono trasmesse ai server Dell Technologies per analizzare i dati e fornire suggerimenti.

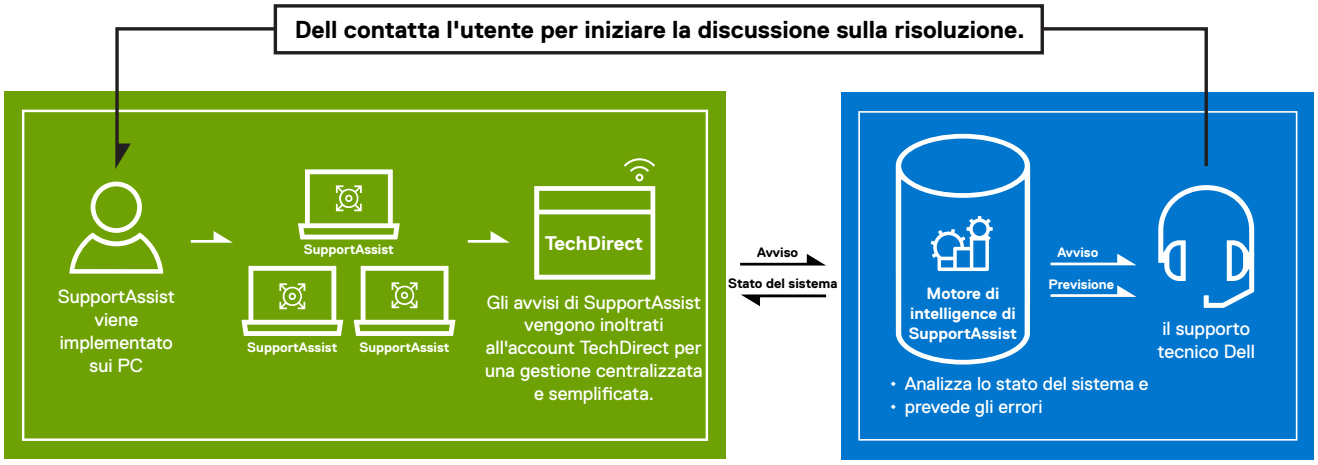
La Guida al deployment contiene un elenco completo dei requisiti di rete, endpoint, porte, firewall o gateway per le procedure di deployment e correzione di SupportAssist. Gli script di correzione sono sviluppati da Dell, nonché testati, firmati e confermati prima dell'esecuzione.

Architettura di SupportAssist



Gestione centralizzata di SupportAssist con TechDirect

Gli avvisi di SupportAssist vengono inoltrati all'account TechDirect di un'organizzazione per assicurare una gestione centralizzata e semplificata. Le organizzazioni che dispongono di un piano di assistenza ProSupport o ProSupport Plus possono anche scegliere di inoltrare automaticamente gli avvisi a Dell Technologies Services.

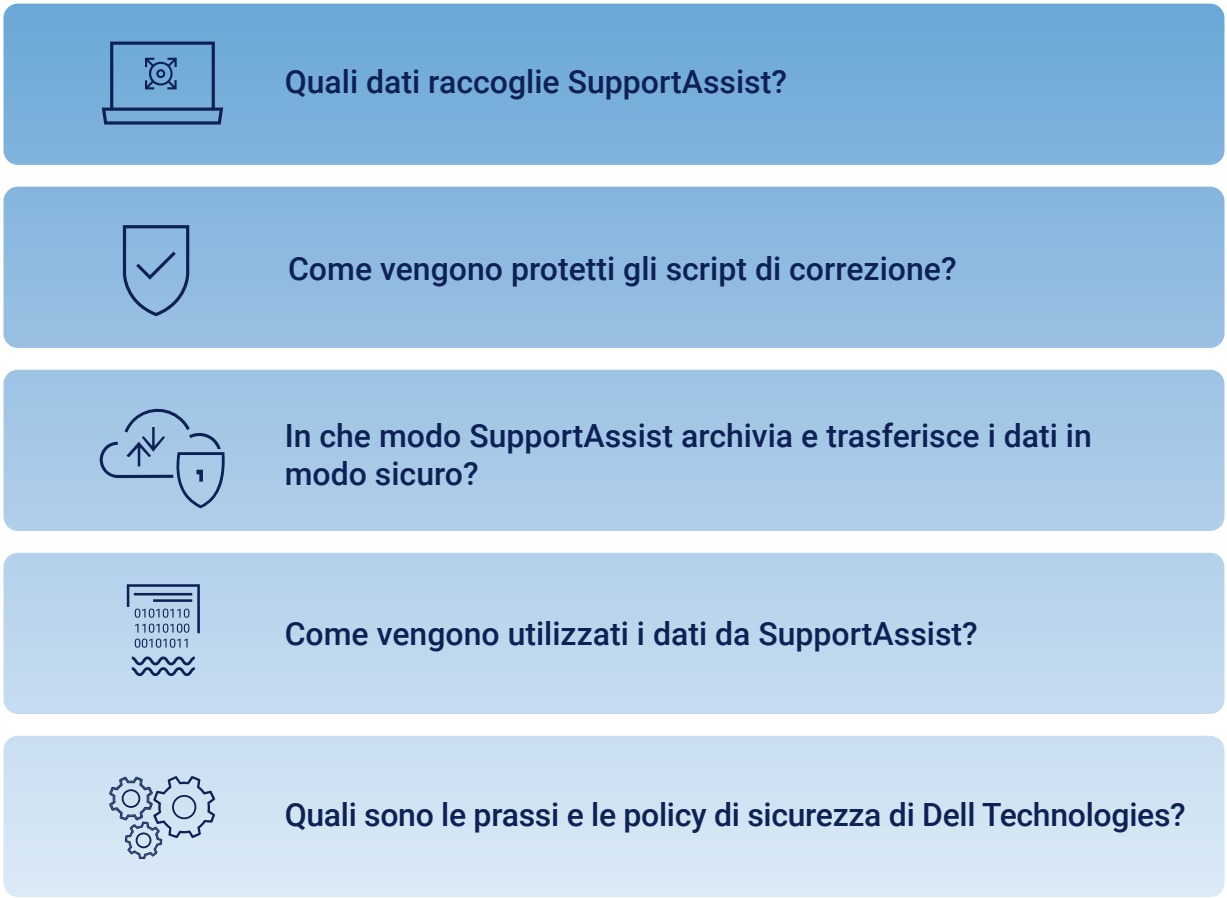


Gestione centralizzata di SupportAssist con TechDirect (continua):

Le informazioni dettagliate di SupportAssist, un componente analitico estremamente utile, raccolgono i dati sull'utilizzo del sistema che possono essere visualizzati all'interno di TechDirect. Questi dati includono l'utilizzo della CPU, lo spazio libero su disco, la capacità massima e la durata della batteria e molte altre informazioni utili. TechDirect è in grado di visualizzare queste informazioni per tutti i sistemi, per i sistemi di uno specifico device group o per un singolo sistema. I clienti possono identificare i problemi relativi alle prestazioni e prendere decisioni aziendali più mirate (ad esempio, in merito alla necessità o meno di sostituire l'hardware o effettuarne l'upgrade).

IV. Sicurezza di SupportAssist

Il CIO o il CSO di un'organizzazione potrebbe avere domande sui tipi di dati raccolti da SupportAssist e sulla modalità di gestione di tali dati. Questa sezione risponde a queste domande e dimostra come SupportAssist raccoglie solo i dati necessari per risolvere i problemi dei clienti, gestendoli con la massima attenzione alla sicurezza.



Quali dati raccoglie SupportAssist?

SupportAssist raccoglie automaticamente i dati necessari per la risoluzione di un problema e li invia in modo protetto al supporto tecnico. Questi dati ci consentono di offrire un'esperienza di supporto adattiva, intelligente e rapida.

Il codice di matricola, necessario per identificare il dispositivo specifico dell'utente finale su cui si sta lavorando, è l'unica informazione aziendale raccolta dai dispositivi. Quando SupportAssist determina che un componente deve essere spedito in modo proattivo, Dell utilizza le informazioni di contatto esistenti, archiviate in modo sicuro (crittografia, criteri di retention, ecc.) sui server Dell Technologies.

Ogni 24 ore, nell'ambito del monitoraggio di routine del sistema, vengono raccolte e inviate le seguenti informazioni:

- **Versione schema:** la versione dello schema utilizzato per il monitoraggio di routine del sistema
- **Versione agent:** la versione di SupportAssist implementata sul sistema
- **Codice di matricola:** l'identificativo univoco del sistema
- **Modello del sistema:** il nome del modello del sistema
- **Informazioni sulla registrazione:** lo stato di registrazione di SupportAssist
- **Versione SO:** la versione del sistema operativo in esecuzione sul dispositivo
- **Versione SP:** il Service Pack del sistema operativo
- **Data UTC:** la data e l'ora in cui le informazioni sul monitoraggio di routine del sistema sono state inviate a Dell Technologies Services
- **Versione BIOS:** la versione del BIOS installata sul sistema
- **Stato:** lo stato dell'avviso in base al livello di gravità, ad esempio, avvertenza
- **Descrizione:** le informazioni sul problema del sistema, ad esempio, utilizzo elevato di CPU
- **Spazio libero su disco rigido:** lo spazio libero disponibile sull'unità disco rigido
- **Utilizzo memoria:** la quantità di memoria di sistema utilizzata
- **Utilizzo CPU:** la quantità di CPU utilizzata
- **Data locale:** la data e l'ora del sistema
- **Data ultimo avvio:** la data e l'ora in cui il sistema è stato riavviato l'ultima volta
- **Data di esecuzione dell'aggiornamento Windows:** la data e l'ora in cui è stato eseguito l'ultimo aggiornamento di Windows sul sistema
- **Numero BSOD nelle ultime 24 ore:** il numero di schermate blu che si sono verificate nelle ultime 24 ore
- **Informazioni sull'avviso:** l'identificativo univoco dell'avviso

Ulteriori informazioni sui dati di monitoraggio del sistema raccolti da un sistema attivo sono disponibili in questa pagina sul sito Dell.com.

Tutte le informazioni vengono trasmesse attraverso canali protetti.

Come vengono protetti gli script di correzione?

Prima di essere caricati sulla piattaforma di correzione, tutti gli script di correzione creati da Dell vengono firmati con i certificati Dell e sottoposti a test e convalida approfonditi per garantire che funzionino come previsto senza produrre risultati imprevisti. Ciò funge da base per verificare l'autenticità dello script prima dell'esecuzione. Per esempio, se un script viene modificato o sostituito sull'endpoint, la verifica della firma del certificato fallirà e SupportAssist bloccherà l'esecuzione dello script. Ciò impedisce l'esecuzione di codice non autorizzato o potenzialmente dannoso. Questi script non possono essere modificati da nessuno al di fuori di Dell, il che garantisce la loro integrità. Si consiglia di testare gli script su un gruppo di PC designato prima di una più ampia distribuzione.

Viene seguito un processo diverso per gli script del flusso di lavoro personalizzato. Quando i clienti caricano i propri script, il sistema di correzione accetta sia script non firmati che script firmati con un certificato del cliente. L'integrità di questi script viene preservata durante il transito verso i PC e quando sono archiviati in stato inattivo. Si consiglia di testare gli script personalizzati su un gruppo specifico di PC prima di una distribuzione più ampia.

TechDirect Connessione e gestione supporta la creazione di siti e gruppi, consentendo ai clienti di convalidare script personalizzati e creati da Dell sui computer di test. Tutte le informazioni presenti nella console di correzione sono protette entro i limiti del tenant in TechDirect, accessibili solo agli utenti con ruoli appropriati assegnati dall'amministratore del tenant. I risultati possono anche essere esportati in un file CSV per un'ulteriore analisi.

In che modo SupportAssist archivia e trasferisce i dati in modo sicuro?

I dati inviati da SupportAssist a Dell Technologies Services sono protetti da crittografia a 256 bit e trasferiti in modo sicuro mediante il protocollo TLS (Transport Layer Security).

Una chiave di crittografia viene generata in runtime su ogni macchina durante l'installazione del pacchetto. La chiave di crittografia viene utilizzata insieme al salt per la crittografia delle informazioni installate. Viene utilizzato un algoritmo standard del settore per la crittografia dei dati inattivi.

In crittografia, il salt è un dato casuale utilizzato come input in una funzione unidirezionale che aggiunge hash ai dati, a una password o passphrase. La funzione principale dei salt è la difesa dagli attacchi con dizionario o dal suo equivalente con hash, ovvero un attacco con tabella arcobaleno pre-elaborato.

Tutte le chiavi di crittografia vengono generate utilizzando un generatore sicuro di numeri casuali. I dati in transito vengono protetti utilizzando il protocollo TLS su HTTPS (Hypertext Transfer Protocol Secure). Tutti gli algoritmi di crittografia sono standard di settore e i dati inattivi sono crittografati.

Il protocollo HTTPS viene utilizzato nelle comunicazioni standard per la trasmissione di feedback dell'utente, eventi di telemetria di diagnostica e query dell'API su Dell.com o Microsoft Azure IoT Hub per le informazioni sul sistema utilizzate nel processo di ripristino. Per l'approccio pub/sub viene utilizzato un protocollo MQTT sicuro.

Il protocollo HTTPS standard viene utilizzato per proteggere le comunicazioni tra il client e l'infrastruttura di back-end durante la trasmissione o il download dei contenuti sul dispositivo dell'utente finale. Il protocollo HTTPS o MQTT sicuro viene utilizzato per proteggere la trasmissione dei dati di telemetria, la comunicazione con un'API back-end su Dell.com o Microsoft Azure IoT Hub e il download di contenuto recuperato da Dell.com.

Tutti i componenti di rete sono posizionati dietro un firewall e vengono gestiti da un team addetto alla sicurezza della rete. Il traffico di rete viene controllato in modo rigoroso. Tutto il traffico in entrata viene trasmesso tramite porte specifiche e inviato solo agli indirizzi di rete di destinazione appropriati. SupportAssist utilizza la larghezza di banda della rete per vari eventi che richiedono connettività all'infrastruttura Dell Technologies Services. La larghezza di banda utilizzata può variare in base al numero di sistemi di destinazione monitorati da SupportAssist. Si prega di fare riferimento al documento "Dati raccolti da PC connessi" per saperne di più sulla media dei dati consumati.

Come vengono utilizzati i dati da SupportAssist?

SupportAssist utilizza i dati raccolti per fornire supporto automatizzato, proattivo e predittivo ai clienti. Se si verifica un problema con un sistema, SupportAssist genera un avviso per consentirne la risoluzione da parte di un agente del supporto tecnico.

SupportAssist utilizza, inoltre, i dati raccolti per prevedere un guasto imminente di un componente, utilizzando un software di intelligenza artificiale basato sui dati raccolti da decine di milioni di sistemi Dell sul campo. Questo avviso predittivo può essere utilizzato per spedire una parte prima che si guasti, determinando un uptime ottimale del sistema e assicurando la protezione dei dati.

Infine, SupportAssist utilizza i dati per rilevare e rimuovere virus e malware dai sistemi degli utenti, ottimizzare le prestazioni del sistema operativo e fornire suggerimenti sugli aggiornamenti del BIOS, dei driver e del firmware.

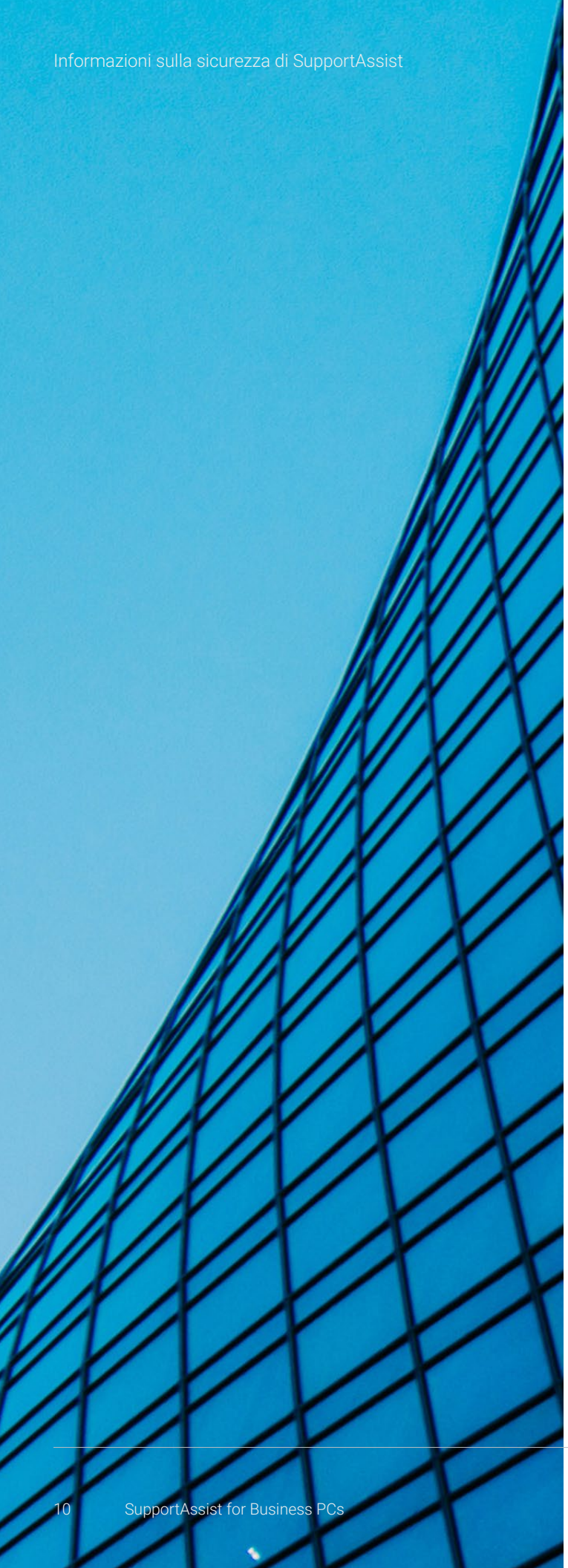
Le app di sistema forniscono informazioni sull'uso del sistema con il componente Insights.

Sicurezza fisica

Dell Technologies Services ospita i dati di SupportAssist, inclusi componenti di sicurezza, applicazioni, sistemi e reti, in un data center negli Stati Uniti progettato per mantenere elevati livelli di disponibilità e sicurezza. I dati di SupportAssist vengono protetti attraverso un'ampia gamma di misure.

L'accesso ai data center dove risiede l'infrastruttura è consentito esclusivamente al personale autorizzato. L'accesso è controllato tramite smart card.

Misure di sicurezza fisica e logica assicurano la protezione dei dati archiviati.



Sicurezza logica

I dati generati da SupportAssist vengono archiviati in conformità all'Informativa sulla privacy Dell.

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

- **Controllo:** i registri dei dispositivi monitorati vengono conservati e sono accessibili esclusivamente dall'infrastruttura e/o dalle applicazioni Dell Technologies Services. Registrano tutti i tentativi di connessione o accesso al sistema operativo o alla console del server web SupportAssist.

Le build gestite dall'IT sono caratterizzate da protezione avanzata mediante i controlli consigliati da Center for Internet Security (CIS) come best practice di sicurezza.

Infine, l'ecosistema SupportAssist sfrutta sia l'high availability locale all'interno del proprio data center che un'infrastruttura identica in un data center distinto. Le uniche eccezioni sono le tecnologie con high availability intrinseca, come i cluster di Big Data e i private cloud.

Per l'analisi dei dati, Dell Technologies Services si avvale di ambienti cloud completamente controllati e gestiti, tra cui private, hybrid e public cloud. Database relazionali, servizi di storage semplici e data warehouse sono tutti crittografati e utilizzano privilegi minimi. Nessun database relazionale è pubblico. I data warehouse sono protetti tramite HTTPS.

Quali sono le prassi e le policy di sicurezza di Dell Technologies?

Sviluppo

Il nostro standard SDL (Secure Development Lifecycle) interno funge da riferimento di base per le organizzazioni di prodotti Dell Technologies e fornisce benchmark essenziali per lo sviluppo sicuro di prodotti e applicazioni. Dell offre un catalogo di controlli SDL definito basato su ISO/IEC 27034 e uno standard basato su NIST Secure Software Development Framework (SSDF). Questi strumenti aiutano i team Dell a realizzare prodotti sicuri per i clienti e a prevenire l'introduzione di vulnerabilità e punti deboli della sicurezza nel software e nell'hardware sviluppati e supportati da Dell. L'adozione di questi controlli è un requisito per i team di progettazione durante lo sviluppo di nuove caratteristiche e funzionalità. Tali controlli comprendono attività di analisi e misure proattive prescrittive incentrate sulle principali aree di rischio.

Le attività di analisi, tra cui la modellazione delle minacce, l'analisi statica del codice, le scansioni e i test di sicurezza, sono parti integranti volte a identificare e mitigare i difetti di sicurezza durante l'intero ciclo di sviluppo. Inoltre, SDL include controlli prescrittivi per assicurare che i team di sviluppo affrontino in modo proattivo problemi di sicurezza specifici, tra cui quelli delineati in standard di settore come Open Web Application Security Project (OWASP) Top 10 e SANS Top 25.

SupportAssist for Business PCs si allinea a questo framework SDL affidabile, impiegando Dell SDL Maturity Model per implementare controlli di sicurezza in conformità agli standard del settore. Il programma DevSecOps protegge i moderni processi di sviluppo e deployment del software in Dell automatizzando i controlli SDL e applicando policy di sicurezza in un'ambiente di integrazione continua e deployment continuo (CI/CD). Questi strumenti CI/CD automatizzano i processi di sviluppo, test e deployment, assicurando che le modifiche al codice siano integrate e testate continuamente nell'ambito del flusso di lavoro di sviluppo.

Gli ingegneri SDL eseguono valutazioni SDL per identificare i problemi e le vulnerabilità di sicurezza nel software e forniscono suggerimenti che consentono ai team di sviluppo di correggere questi risultati. Tutto questo offre visibilità sulla maturità delle nostre procedure e sul profilo di sicurezza dei nostri software e hardware.

Il processo include:

- Valutazione delle vulnerabilità con test di penetrazione.
- Test di sicurezza di terze parti condotti da rinominati fornitori, come Secureworks.
- Valutazione di soluzioni di gestione dell'autenticazione, dell'autorizzazione e delle identità.
- Scansione approfondita di tutte le librerie e tutti i componenti di terze parti mediante strumenti di analisi della composizione software leader del settore.
- Comunicazione di Dell Security Advisory per miglioramenti specifici della sicurezza.
- Rigorosa classificazione dei dati in collaborazione con la nostra organizzazione Global Security, allineando le iniziative in ambito di privacy e sicurezza al fine di proteggere i dati elettronici.
- Esecuzione di controlli di sicurezza e procedure di governance sulle applicazioni.

GDPR

Dell ha implementato misure volte a garantire che disponiamo dei processi e delle procedure necessari per ottemperare ai nostri obblighi ai sensi del GDPR. Dell tiene traccia degli sviluppi delle leggi sulla privacy in tutto il mondo e garantisce la conformità agli obblighi applicabili previsti dalla legislazione sulla privacy pertinente. Se Dell agisce in qualità di responsabile del trattamento, lo fa in base a un modulo concordato di comune accordo o in altro modo a un modulo standard del Contratto di trattamento dei dati. Per ulteriori informazioni, visita i seguenti link:

- Riepilogo dei controlli e delle dichiarazioni aziendali sulla sicurezza delle informazioni del GDPR di Dell
- L'impegno di Dell a favore della conformità al GDPR
- Domande frequenti sulla conformità di Dell per i clienti di Dell Technologies

Processi sicuri e collaudate procedure di settore contribuiscono alla sicurezza di SupportAssist.

Test di convalida della sicurezza

Valutazioni della sicurezza di terze parti vengono condotte periodicamente per l'applicazione SupportAssist e per la relativa infrastruttura di supporto.

Le valutazioni dell'applicazione includono sicurezza a livello di API e trasporto dei dati, analisi statica e dinamica del codice sorgente, controlli incrociati OWASP (Open Web Application Security Project) e librerie di terze parti.

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

Gestione delle modifiche

Il processo di gestione delle modifiche Dell Technologies segue le best practice di ITIL Foundation, su richiesta del nostro comitato aziendale addetto alla gestione delle modifiche. Tutte le modifiche vengono gestite tramite ticket di richiesta di modifiche. Le persone che accedono al nostro sistema per avviare modifiche sono tenute a seguire la formazione ITIL e ad acquisire familiarità con SDL. Tutti gli aggiornamenti e gli upgrade applicati all'infrastruttura back-end sono sottoposti a controllo delle versioni per assicurare livelli appropriati di monitoraggio e tracciabilità. Il team impiega un processo automatizzato per applicare nuove build o revocare eventuali build e hotfix distribuiti.

Ogni versione promossa a Dell.com/support contiene informazioni sulle modifiche introdotte con eventuali limitazioni note.

Tutte le nuove funzioni e modifiche vengono preparate dal nostro team di gestione dei prodotti e classificate in ordine di priorità attraverso un piano di record e un processo di gestione delle modifiche.

Autenticazione

SupportAssist utilizza Dell MyAccount per l'autenticazione con l'infrastruttura Dell Technologies Services, la chiave simmetrica casuale dell'applicazione, JWT e i gruppi di accesso OS per l'autenticazione on-the-box.

Ai gruppi che hanno accesso ai componenti di SupportAssist, ad esempio il team di amministrazione del database e il team di supporto operativo, vengono assegnati compiti e diritti di accesso distinti. Tutti gli aggiornamenti applicati all'ambiente di produzione sono sottoposti a un processo di controllo delle modifiche definito che comprende verifiche e bilanciamenti.

Community attenta alla sicurezza

Dell offre un curriculum di formazione sulla sicurezza in base ai ruoli per istruire i dipendenti nuovi ed esistenti sulle best practice di sicurezza specifiche per il lavoro e su come utilizzare le risorse pertinenti. Dell Technologies si impegna a creare una cultura attenta alla sicurezza in tutta la community. Inoltre, la community di sviluppatori partecipa al programma Security Champion di Dell, ideato per promuovere la sicurezza shift-left nelle procedure di sviluppo del software.

Reporting sugli incidenti

In Dell Technologies, tutti i dipendenti sono tenuti a segnalare tempestivamente eventuali attività sospette, problemi di sicurezza informatica o minacce al nostro Computer Security Incident Response Team (CSIRT) tramite e-mail all'indirizzo security@dell.com.

Risposta alle vulnerabilità

Dell Technologies si impegna a ridurre al minimo i rischi associati alle vulnerabilità della sicurezza nei nostri prodotti, applicazioni e servizi cloud. Per assicurare procedure tempestive di risposta alle vulnerabilità, Dell si attiene alle linee guida indicate nel Vulnerability Response Standard (VRT) di Dell Technologies. Dell partecipa attivamente a diverse iniziative della community, tra cui il Forum of Incident Response and Response Teams (FIRST) e il Software Assurance Forum for Excellence in Code (SAFECode). I processi e le procedure di Dell sono in linea con il FIRST PSIRT Services Framework, nonché con altri standard, tra cui ISO/IEC 29147:2018 e ISO/IEC 30111:2019.

Dell Technologies si impegna a gestire le vulnerabilità dei propri prodotti, applicazioni e servizi cloud nel più breve tempo commercialmente ragionevole. Le tempistiche esatte possono variare a seconda della vulnerabilità specifica e del suo impatto, ad esempio la complessità dell'impatto o dell'iniziativa di vulnerabilità da correggere. Il team PSIRT (Product Security Incident Response) coordina la risposta e la divulgazione di tutte le vulnerabilità dei prodotti che ci vengono segnalate. Tutte le divulgazioni sulle vulnerabilità dei prodotti Dell Technologies sono disponibili online alla pagina Avvisi di sicurezza, preavvisi e risorse di Dell. Ulteriori informazioni sulle procedure di risposta alle vulnerabilità Dell sono disponibili alla pagina Policy di risposta Dell alle vulnerabilità.

Affiliazioni di settore

Dell Technologies partecipa a diversi gruppi del settore per collaborare con altri principali fornitori alla definizione, all'evoluzione e alla condivisione delle best practice per la sicurezza dei prodotti e promuovere metodologie di sviluppo sicuro. Di seguito sono indicati alcuni esempi di collaborazione nel settore:

- Dell Technologies ha cofondato e attualmente presiede il consiglio di amministrazione del Software Assurance Forum for Excellence in Code (SAFECode). Tra gli altri membri del consiglio figurano rappresentanti di Microsoft, Adobe, SAP, Intel, Siemens, CA e Symantec. I membri di SAFECode condividono e pubblicano procedure e corsi di formazione in ambito di Software Assurance.

Leader del settore nella definizione delle best practice per la sicurezza dei prodotti e nella promozione di metodologie di sviluppo sicuro.

Affiliazioni di settore (continua)

- Dell Technologies è membro attivo del Forum of Incident Response and Security Teams (FIRST). FIRST è un'organizzazione di eccellenza e leader globale riconosciuto in ambito di risposta agli incidenti e alle vulnerabilità.
- Dell partecipa in modo attivo all'Open Group Trusted Technology Forum (OTTF). OTTF guida lo sviluppo di un programma e di un framework globali per l'integrità della supply chain.
- 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.

Standard di sicurezza del settore

- I dipendenti Dell partecipano attivamente agli organismi di standardizzazione e ai consorzi del settore che si occupano di sviluppare standard e di definire procedure di sicurezza per l'intero settore, tra cui:
- Cloud Security Alliance (CSA)
- Forum of Incident Response and Security Teams (FIRST)
- The Open Group
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

Dell Technologies dispone della certificazione ISO 9001. Dell conduce regolarmente audit trimestrali e revisioni della conformità per tutti i suoi centri di sviluppo e produzione.

V. Conclusioni

La tecnologia di connettività SupportAssist offre funzionalità intelligenti di automazione e correzione per assicurare il massimo uptime della flotta di computer desktop e notebook Dell di un'organizzazione. Dell Technologies Services è in grado di fornire questa tecnologia all'avanguardia con un livello di sicurezza ottimale, concentrandosi su processi, trasmissione e storage dei dati sicuri.

Per eventuali domande e ulteriori informazioni, è possibile visitare la pagina all'indirizzo **Dell.com/SupportAssist**

[1] Per i requisiti e i sistemi supportati, consultate la nostra guida utente (versione di SupportAssist for Home PCs per uso personale) o la guida dell'amministratore (versione di SupportAssist for Business PCs per la gestione della flotta di PC) e cliccate su "PC supportati". Le funzionalità proattive e predittive variano a seconda del piano di assistenza attivo e delle regole aziendali Dell Technologies. Per le funzionalità di ProSupport Suite for PCs consultate la nostra guida dell'amministratore e cliccate sulla voce relativa a funzionalità di connessione e gestione e piani di assistenza Dell. Per le funzionalità di Dell Care Suite, Premium Support Suite o Alienware Care Suite per PC, consultate la guida utente e cliccate sulla voce relativa a funzionalità di SupportAssist e piani di servizio Dell.

[2] Dati basati su un'analisi Dell, dicembre 2023.