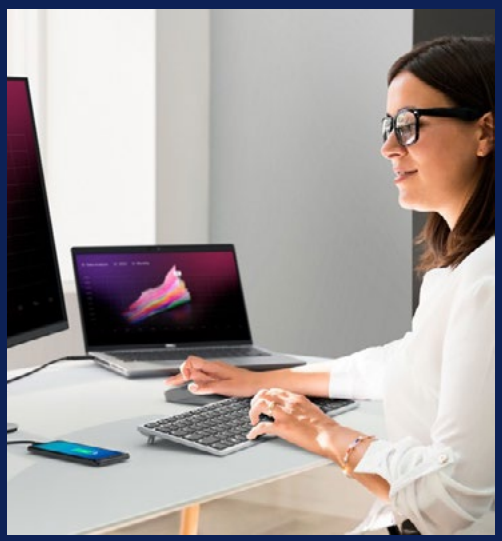
DELL Technologies

Strategia completa

Come proteggere la forza lavoro che utilizza l'AI con Dell Technologies, Microsoft e Intel.



Windows 11

intel

Executive Summary

Il passaggio al lavoro ibrido ha portato con sé nuove complessità e nuovi vettori di attacco, con endpoint, reti e cloud che espandono le superfici di attacco. La corsa per adottare l'AI generativa alza ulteriormente la posta in gioco, introducendo nuove considerazioni sulla sicurezza, tra cui la perdita di dati e proprietà intellettuale, nonché attacchi contestuali ad alta velocità.

Inoltre, gli hacker ora impiegano tecniche sofisticate che prendono di mira diversi livelli dello stack informatico, integrandosi con processi di sistema validi. Alcuni metodi consentono agli hacker di ottenere persino l'accesso con privilegi e disabilitare le protezioni software senza essere minimamente rilevati.

L'unione fa la forza...

Nessun provider è in grado di risolvere tutti questi problemi da solo. Ed è per questo che Dell, Microsoft e Intel hanno strategicamente unito le loro forze per liberare le organizzazioni da questo onere.

Il nostro approccio olistico alla sicurezza integra funzionalità "below-the-OS" (al di sotto del sistema operativo) basate su hardware per la protezione dagli attacchi con le difese silicon-based di Intel, capaci di arrivare ai livelli più profondi del dispositivo.

In questo modo, Windows 11, i moderni dispositivi Dell e il software lavorano in perfetta sinergia per ridurre la superficie di attacco, proteggere l'integrità del sistema e preservare sia gli utenti che i dati più importanti.

La collaborazione è alla base del successo.

La sicurezza unica e integrata di Dell Technologies comprende tutte le innovazioni relative alla sicurezza dei nostri partner Intel e Microsoft, così da proteggere la forza lavoro ibrida dalle minacce in continua evoluzione.

Solo il 33% delle organizzazioni IT usa una strategia di sicurezza olistica end-to-end che integra protezioni basate sia sull'hardware che sul software.

Fonte: Dell Innovation Index, 2023

Argomenti trattati in questo documento

Elementi alla base della sicurezza

Secure Development Lifecycle

Dell Technologies, Microsoft e Intel lavorano insieme per garantire sicurezza a ogni livello, dal chip al cloud. I Dell Trusted Device, ovvero i PC commerciali più sicuri del settore*, sono l'esempio perfetto di questa collaborazione.

Sicurezza della supply chain

Le protezioni implementate lungo la supply chain garantiscono la sicurezza dei dispositivi dopo che questi hanno lasciato la fabbrica.

* Dati basati su analisi interne Dell, settembre 2022. Non tutte le funzioni sono disponibili con tutti i PC. Alcune funzioni sono acquistabili in aggiunta.

Framework di difesa completo che abilita la sicurezza Zero Trust

Sicurezza basata su AI

Sfrutta l'AI per automatizzare la protezione degli utenti e offrire innovative soluzioni di sicurezza pronte all'uso.

Sicurezza al di sotto del sistema operativo

Le funzionalità di sicurezza basate su hardware proteggono i dispositivi dalle minacce indirizzate ai livelli di base.

Sicurezza al di sopra del sistema operativo

Le tecnologie di sicurezza basate su software e le protezioni basate su silicio sono entrambe fondamentali per la totale sicurezza dei dispositivi.

Sicurezza di Windows 11

Protezione preconfigurata con livelli di hardware e software strettamente integrati tra loro su sistema operativo, applicazioni, identità e cloud.

Supporto su base continuativa

Con Dell, Microsoft e Intel, le soluzioni sono sempre protette grazie all'applicazione di patch per eliminare le vulnerabilità e all'aggiornamento della sicurezza silicon-based all'interno del sistema operativo.

Se gli endpoint sono deboli, la rete aziendale non è sicura

Ogni tanto, importanti aziende a livello globale subiscono gravi violazioni della sicurezza e l'esposizione pubblica negativa che ne deriva compromette in modo serio la loro reputazione. È importante che imprenditori e professionisti della sicurezza mantengano sempre alto il livello di attenzione, dal momento che anch'essi sono esposti ai rischi, che si tratti di vulnerabilità non individuate nei dispositivi o di vulnerabilità sconosciute a livello software. Si può avere fiducia nel proprio team IT per quanto riguarda la protezione delle reti e l'implementazione di pratiche per la sicurezza dei dati, ma come si può avere la certezza che tutti gli endpoint e tutte le applicazioni su cui si fa affidamento per la propria attività siano sicure in assenza di una supervisione in fase di produzione o sviluppo?

Dell, Microsoft e Intel sanno perfettamente che armonizzare le tecnologie di sicurezza hardware e software è l'unico modo per proteggere in modo affidabile dispositivi e reti aziendali. I nostri team hanno lavorato insieme per creare funzionalità di sicurezza hardware e software strettamente integrate, ma altri provider potrebbero non aver effettuato questo tipo di investimento.

L'approccio comune ma al tempo stesso imperfetto all'integrità dei dispositivi vuole infondere un falso senso di sicurezza attraverso soluzioni basate esclusivamente sul software, senza però affrontare le vulnerabilità a livello hardware. È fondamentale che i responsabili aziendali comprendano i limiti di questa strategia. Affidandosi unicamente al software per proteggere l'ambiente aziendale, l'hardware su cui è eseguito il software rimane esposto e vulnerabile a possibili attacchi. In sostanza, se l'hardware non è sicuro, le tecnologie e le applicazioni di sicurezza in esecuzione su di esso non possono essere protette.

Altri provider tentano di creare un "recinto" per proteggere i dispositivi. In questo caso, però, le limitazioni sono integrate nelle applicazioni e nei servizi, limitando la flessibilità degli utenti. Anche se potrebbe avere senso a livello consumer, una scelta del genere limita la possibilità di utilizzare al meglio i dispositivi, peggiorando ulteriormente la situazione in un contesto commerciale. Questo approccio, inoltre, porta gli autori di attacchi informatici ad attaccare e violare sempre più spesso i sistemi, rivelando le vulnerabilità nelle configurazioni comuni.

In poche parole, quello che funziona per i dispositivi direct-to-consumer spesso non funziona in un ambiente commerciale, che rappresenta un obiettivo più interessante per gli autori di attacchi informatici.

Ecco perché Dell, Microsoft e Intel adottano un approccio olistico e diversificato per quanto riguarda la sicurezza.

Se gli endpoint sono deboli, la rete aziendale non è sicura

Dell, Microsoft e Intel forniscono sicurezza integrata basata su hardware

Le complessità e le problematiche associate alla protezione dei dispositivi e delle reti sono motivo di grande preoccupazione. Ed è proprio qui che entriamo in gioco. La nostra mission, infatti, è fornire ai clienti dispositivi incentrati sulla sicurezza, per consentire loro di focalizzarsi su ciò che conta davvero: la gestione delle attività aziendali.

Iniziata decenni fa, la collaborazione tra Dell, Microsoft e Intel nell'ambito della progettazione ha da sempre come obiettivo quello di proteggere i dati dei clienti, specialmente nel mercato business-to-business. Grazie alla sua partnership con Microsoft e Intel, Dell si è costruita una solida reputazione come fornitore di riferimento di dispositivi per dipendenti di aziende di tutte le dimensioni e in ogni mercato.

Ma cosa racchiude al suo interno un dispositivo commerciale Dell? Dentro troviamo funzioni sapientemente combinate, tecnologie, strumenti e policy per l'intero ciclo di vita dei PC commerciali che forniscono sicurezza end-to-end ai clienti e alle loro aziende.

Sicurezza fin dalla progettazione

Per ridurre al minimo la superficie di attacco e garantire la protezione dei dispositivi commerciali, Dell, Microsoft e Intel non si limitano a prendere in considerazione solo le minacce attuali quando progettano i sistemi futuri.

Protezione in transito

Abbiamo attuato tecnologie e policy che contribuiscono a proteggere l'integrità dei dispositivi prima che giungano nelle mani dell'utente, garantendo la sicurezza durante le fasi di approvvigionamento, assemblaggio e consegna dei componenti.

Difesa contro le minacce in continua evoluzione

Utilizziamo la sicurezza basata su hardware resa possibile dalle tecnologie Dell Trusted Device e dalle funzionalità Intel® Hardware Shield per rafforzare le difese dei dispositivi attraverso un framework di prevenzione, rilevamento e risposta. Inoltre, Dell, Microsoft e Intel dispongono di team addetti alla sicurezza impegnati a controllare i propri prodotti e a individuare nuove vulnerabilità prima che lo facciano gli autori degli attacchi informatici, intervenendo in modo tempestivo con l'installazione di patch per garantire la sicurezza necessaria.

In questo white paper vedremo come Dell, Microsoft e Intel hanno sviluppato insieme piattaforme per PC commerciali con sicurezza integrata ai livelli più profondi per proteggere i dispositivi durante il loro intero ciclo di vita, durante il loro successivo aggiornamento e non solo.

La protezione delle nostre piattaforme inizia davanti a una lavagna

Pianificazione, valutazione e analisi

Prima di progettare piattaforme, chipset e software innovativi, gli esperti Dell, Microsoft e Intel definiscono i rigorosi parametri che una piattaforma deve includere per essere considerata sicura, soddisfare le esigenze di sicurezza future e rispettare le normative. Il processo inizia con una tavola rotonda dove vengono stabiliti i potenziali rischi futuri per la sicurezza e la privacy, nonché le attività necessarie per mitigarli. Questo serve a definire gli obiettivi in base ai quali valuteremo le nostre architetture.

Con le informazioni raccolte, i team addetti alla sicurezza di Dell, Microsoft e Intel sviluppano modelli di minacce per ricreare comportamenti malevoli e testare l'architettura concettuale in modo da individuare potenziali vulnerabilità e falle che gli hacker potrebbero sfruttare. Questo approccio si è dimostrato particolarmente vantaggioso, in quanto fornisce significativi miglioramenti nell'individuazione e nella riduzione delle potenziali vulnerabilità nella progettazione di BIOS, firmware e hardware.

Progettazione incentrata sulla sicurezza

Una volta completate le valutazioni delle minacce e creati i modelli per definire la superficie delle minacce stesse e i punti in cui è necessario concentrare i test, gli ingegneri iniziano a sviluppare il codice del prodotto. Gli obiettivi di sicurezza definiti nel passaggio precedente forniscono indicazioni durante questa fase di sviluppo e fungono da criterio per stabilire se il prodotto potrà effettivamente soddisfare le esigenze dei nostri clienti.

La protezione delle nostre piattaforme inizia davanti a una lavagna

Verifica e test

Dopo aver perfezionato il codice al punto da soddisfare gli obiettivi di sicurezza stabiliti all'inizio del ciclo di vita dello sviluppo, il prodotto viene sottoposto a test rigorosi.

Questi test in genere iniziano con revisioni del secure code e l'analisi del codice statico, un processo automatizzato che utilizza strumenti speciali per individuare e correggere i difetti. Alcuni prodotti con codice più complicato passano quindi a un processo di revisione manuale, in cui gli esperti di sicurezza esaminano riga per riga il codice in modo da individuare eventuali errori precedentemente non rilevati e assicurarsi che sia stato progettato correttamente.

Infine, team di hacker esperti eseguono test di penetrazione e altre simulazioni di attacco per rilevare potenziali vulnerabilità non individuate nelle fasi precedenti. I risultati vengono nuovamente mitigati in base al rischio, in modo da documentare e correggere eventuali altre esposizioni individuate.

Rilascio e post-rilascio

Dopo aver testato il prodotto in base a criteri rigorosi e stabilito che soddisfa o supera gli obiettivi di sicurezza definiti nella fase iniziale, questo è pronto per essere rilasciato sul mercato. Tuttavia, le fasi di rilascio e post-rilascio rappresentano solo una parte del ciclo di vita dello sviluppo sicuro. Per Dell e Intel, la sicurezza delle nostre piattaforme è un impegno costante. I nostri team lavorano per individuare le vulnerabilità prima che possano essere sfruttate dagli autori degli attacchi informatici, quindi sviluppano e rilasciano gli aggiornamenti di sicurezza per risolvere tali falle.

Un esempio del nostro impegno verso la sicurezza end-to-end è dato dall'investimento in una supply chain sicura tra l'assemblaggio e la consegna del dispositivo: la supply chain, infatti, è considerata uno dei vettori di attacco in più rapida crescita tra i malintenzionati. Nella sezione successiva, illustreremo il modo in cui Dell e Intel riducono i rischi lungo le supply chain per garantire che il dispositivo consegnato ai clienti sia protetto fin dal primo avvio.

Garanzia della supply chain come elemento fondamentale per la sicurezza dei dispositivi

Sono tanti gli eventi che possono verificarsi tra il momento in cui un componente o un dispositivo lascia la fabbrica e il suo arrivo a destinazione. Ogni fase della supply chain rappresenta un nuovo vettore che espone dipendenti, attività aziendali e clienti a potenziali attacchi. Dell e Intel hanno sviluppato strumenti, tecnologie e processi per garantire la sicurezza dei propri prodotti prima della consegna ai clienti ed eseguire l'auto-verifica dell'autenticità dei dispositivi prima della distribuzione ai dipendenti.

Approvvigionamento

Dell si avvale di un rigoroso processo di screening dei partner per garantire la qualità e la sicurezza dei dispositivi e dei relativi componenti. I partner, inoltre, sono sottoposti regolarmente a controlli per assicurarsi che rispettino tutti gli standard di sicurezza della supply chain.

Produzione

Oltre a rispettare gli standard di sicurezza della supply chain di Dell, le aziende che producono i nostri dispositivi spesso testano i componenti durante la produzione per evitare che prodotti contraffatti entrino nella supply chain. Per ridurre ulteriormente questo rischio, sui componenti ad alto rischio contenenti informazioni quali fornitore, numero parte, paese di origine e data di produzione vengono applicate etichette PPID (Piece Part Identification Number) univoche, in modo che Dell possa identificare, autenticare, monitorare e convalidare tali componenti eavere così la certezza che il cliente riceva esattamente ciò che è stato spedito.

Distribuzione

Durante il trasporto, Dell prevede una serie di livelli di sicurezza fisica a scopo di protezione, tra cui sigilli antimanomissione, meccanismi di blocco delle porte e dispositivi di tracciamento progettati per rilevare eventuali manomissioni interne dei dispositivi Dell in questa fase.

I dispositivi Dell sono dotati anche di tecnologie di rilevamento delle manomissioni. Le soluzioni Dell Technologies Safe SupplyChain comprendono controlli di sicurezza e integrità della supply chain, ad esempio sigilli antimanomissione e cancellazioni del disco rigido a livello NIST, al fine di garantire una base pulita per la creazione dell'immagine aziendale.

Garanzia della supply chain come elemento fondamentale per la sicurezza dei dispositivi

Verifica

I dispositivi commerciali Dell sono provvisti di certificati della piattaforma con firma crittografica che acquisiscono gli attributi della piattaforma durante la produzione, l'assemblaggio, i test e l'integrazione. Tali attributi vengono quindi collegati tramite crittografia a un dispositivo specifico utilizzando la tecnologia Trusted Platform Module (TPM) come root of trust a livello hardware.

Dell ha implementato i certificati della piattaforma Trusted Computing Group all'interno della soluzione Dell Secured Component Verification (SCV) per i PC commerciali con processori Intel. SCV fornisce all'IT certificati di inventario con firma crittografica per i dispositivi Dell supportati. Con strumenti di auto-verifica sicuri, SCV garantisce la completa integrità dell'hardware durante il transito verso gli ambienti IT e consente ai clienti di verificare che i PC commerciali e i componenti chiave Dell arrivino come sono stati effettivamente ordinati e realizzati.

Da molti anni, anche Intel offre ai vendor trasparenza e tracciabilità della supply chain digitale di base. Intel®Transparent Supply Chain (Intel®TSC) fornisce certificati della piattaforma TCG e dati relativi ai componenti per supportare le piattaforme basate su Intel utilizzando un'API cloud disponibile per l'IT tramite il portale web Intel®TSC. Anche se Dell e Intel hanno scelto di implementare soluzioni indipendenti, i certificati della piattaforma TCG sono un elemento comune tra Intel®TSC e Dell SCV. Questo punto di contatto fornisce la compatibilità e l'interoperabilità di cui gli acquirenti aziendali e della pubblica amministrazione hanno bisogno per implementare i certificati della piattaforma TCG e avere così migliori garanzie di sicurezza della supply chain digitale per i dispositivi basati su Intel.

Framework di difesa completo che abilita la sicurezza Zero Trust

Le organizzazioni impegnate ad accrescere la propria maturità in termini di sicurezza informatica stanno mettendo a punto una roadmap che consenta loro di identificare nuovi modi per ridurre la superficie di attacco, rilevare e contrastare le minacce informatiche e implementare soluzioni per eseguire il ripristino dagli attacchi informatici, il tutto con funzionalità che abilitano la Zero Trust.

Per fare fronte a minacce informatiche sempre più sofisticate, Dell utilizza le funzionalità di sicurezza integrate nelle nostre soluzioni e nelle soluzioni dei partner, tra cui Microsoft e Intel, al fine di aiutare i clienti a implementare una strategia Zero Trust in linea con i loro obiettivi aziendali.

Il 77%

non ha ancora valutato/ sviluppato un'architettura Zero Trust*

* Dell Technologies, Innovation Index, 2023: https://www.dell.com/en-us/dt/perspectives/innovation-index.htm

Architettura completamente integrata per semplificare notevolmente l'adozione della Zero Trust da parte della forza lavoro

Dell, Microsoft e Intel collaborano per offrire ai clienti un ambiente di lavoro ibrido sicuro e senza problemi, nel pieno rispetto dei tre principi della Zero Trust:

1. Verifica esplicita

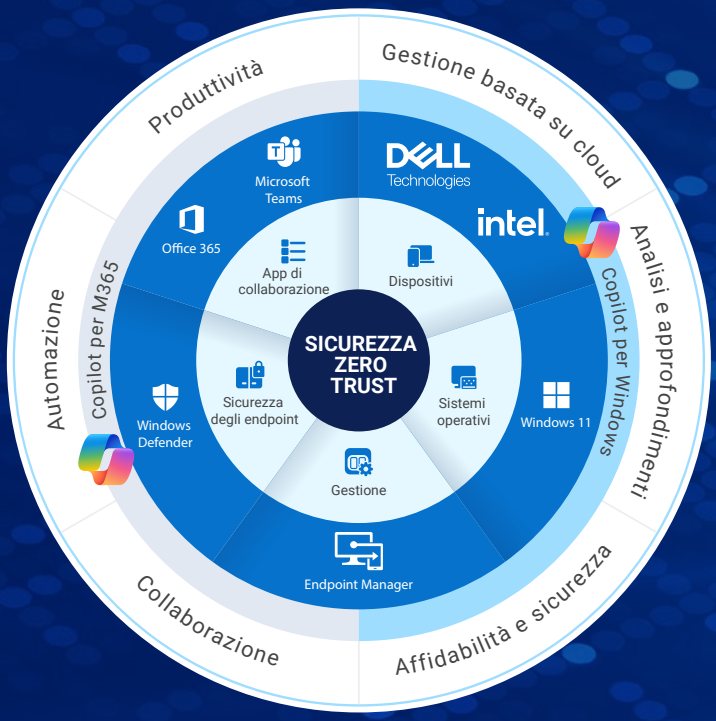
Autenticazione e autorizzazione sempre eseguite in base a tutti i data point disponibili, tra cui identità dell'utente, posizione, stato del dispositivo, servizio o carico di lavoro, classificazione dei dati e anomalie.

2. Utilizzo dell'accesso con privilegi minimi

Applicazione di un limite all'accesso degli utenti con i modelli Just-In-Time e Just-Enough-Access (JIT/JEA), i criteri adattivi basati sul rischio e la protezione dei dati per preservare sia la produttività sia i dati.

3. Presunta violazione (Assume Breach)

Approccio operativo che riduce al minimo il raggio di esplosione e l'accesso ai segmenti, verifica della crittografia end-to-end e utilizzo dell'analisi per ottenere visibilità, favorire il rilevamento delle minacce e migliorare le difese.



Le nostre soluzioni congiunte permettono alle organizzazioni di implementare un modello di sicurezza Zero Trust verificando ogni tentativo di accesso e applicando rigorose policy di sicurezza in base all'identità, allo stato del dispositivo, alla posizione e al livello di rischio, al fine di ridurre il rischio di accesso non autorizzato e limitare l'impatto delle violazioni della sicurezza.

Ciò è possibile integrando:

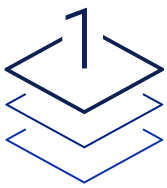
Sicurezza a livello del BIOS/firmware per PC commerciali Dell, sicurezza dell'hardware, garanzia della supply chain, software di gestione delle minacce (EDR, XDR e VDR) e software di protezione dei dati in rete/su cloud in combinazione con Intel® Hardware Shield solo sulla piattaforma Intel vPro®.

Suite completa di strumenti e tecnologie Microsoft per la gestione delle identità e degli accessi, la sicurezza degli endpoint, la sicurezza della rete, la protezione dei dati, la threat intelligence, l'analisi della sicurezza, l'applicazione delle policy e il monitoraggio continuo con risposta (tra cui Azure Active Directory, Microsoft Defender for Endpoint, Azure Firewall, Azure Information Protection, Microsoft Threat Intelligence, Azure Sentinel, Microsoft Endpoint Manager e Microsoft Security Center).

Sicurezza basata su AI

Innovative soluzioni di sicurezza basate su AI pronte all'uso

Dell, Microsoft e Intel sfruttano l'intelligenza artificiale per automatizzare la protezione degli utenti, offrendo insieme innovative soluzioni di sicurezza pronte all'uso. Progettate per impedire e rilevare gli attacchi altamente sofisticati di oggi, queste misure rivoluzionarie integrano sicurezza basata su hardware, crittografia avanzata e protezione contro i malware, con tutta la potenza dei processori Intel® Core™ Ultra su piattaforma Intel vPro® e sistema operativo Windows 11 Pro (alla base dei moderni dispositivi Dell). Grazie a questa sinergia, è possibile ridurre in modo significativo la superficie di attacco attraverso l'implementazione di difese a più livelli incentrate su tre aree principali:



1. BIOS e firmware (below-the-OS):

- Frutto della collaborazione tra Dell e Intel, Dell SafeBIOS è l'efficace meccanismo di difesa contro gli attacchi al BIOS e al firmware che prevede la verifica off-host per assicurare l'integrità del BIOS utilizzando il firmware sulla piattaforma Intel vPro®.
- L'innovativa piattaforma Intel vPro® riduce fino al 70% la superficie di attacco fisica rispetto ai dispositivi di quattro anni fa*
- Integrando la suite di protezioni in perfetta sinergia tra loro, i dispositivi Dell con piattaforma Intel vPro® hanno ottenuto la certificazione Windows 11 Secured Core PC Level 3.
- L'Intel System Security Report, ad esempio, garantisce al sistema operativo che il processo di avvio è stato eseguito in tutta sicurezza, assicurando l'integrità fin dall'inizio.
- Queste protezioni sono intrinseche e subito pronte all'uso.

2. Protezione dei dati e delle applicazioni:

- Per proteggere le credenziali utente vengono implementate funzionalità avanzate quali l'isolamento delle credenziali stesse (agevolato da Windows Hello tramite le tecnologie di virtualizzazione Intel).
- Grazie alla crittografia totale della memoria a più chiavi, le macchine virtuali di Windows 11 sono dotate di memoria crittografata, isolando efficacemente i processi e i dati associati.
- Queste misure proattive sono preconfigurate per essere subito utilizzate oppure possono essere regolate tramite il Centro di Sicurezza di Windows.

3. Rilevamento delle minacce avanzate:

- La tecnologia Intel® TDT (Threat Detection Technology) è l'unica soluzione di rilevamento delle minacce basata su AI a livello di silicio in grado di contrastare gli attacchi ransomware e di cryptojacking.
- Poiché il ransomware fa grande affidamento sulla CPU per crittografare i contenuti aziendali critici, la tecnologia Intel TDT sfrutta il rilevamento delle minacce basato su AI per analizzare la telemetria della CPU e individuare gli indicatori di attacco, segnalando prontamente i processi malevoli affinché intervengano i software di sicurezza come Microsoft Defender per agevolarne la quarantena o l'interruzione.

*13th Gen Intel® Core™ Processor Attack Study Report

Sicurezza basata su AI

Nell'ambito della nostra collaborazione offriamo anche la scansione accelerata della memoria per il rilevamento precoce dei malware fileless, aggiungendo un ulteriore livello di sicurezza per contrastare gli attacchi malware. La partnership con Microsoft Defender e Intel TDT ci permette di ottimizzare i processi di scansione con uso intensivo delle risorse di elaborazione scaricandoli sulla GPU, in modo da liberare la GPU e garantire così produttività senza interruzioni. In caso di potenziale attacco, la GPU comunica in modo proattivo con MSFT Defender, per un approccio alla scansione ancora più completo.

Questa funzione **fornisce vantaggi alle organizzazioni** in **tre modi:**

Riduzione del volume di attacchi fileless, ormai diventati il metodo di ingresso predominante per vari attacchi informatici.

Rilevamento precoce degli attacchi ransomware e di altre minacce malevoli nella fase iniziale di accesso alla memoria.

Mantenimento di un'esperienza utente di altissima qualità mentre sono in corso le scansioni per la protezione della sicurezza.

Sfruttando la scansione accelerata della memoria, le organizzazioni potenziano la loro difesa contro le minacce informatiche in continua evoluzione, garantendo al contempo livelli ottimali di efficienza operativa e produttività utente.

In poche parole, dalla collaborazione tra Dell, Microsoft e Intel nascono soluzioni di sicurezza complete che comprendono protezione basata su hardware, processi di avvio sicuri, sicurezza dei dati e delle applicazioni e funzioni avanzate di rilevamento delle minacce. Ogni aspetto di queste soluzioni è progettato fin nei minimi dettagli per contrastare le minacce in continua evoluzione di oggi.

Tecnologie di sicurezza integrate come mezzo per prevenire, rilevare e contrastare le minacce

Sicurezza olistica significa andare oltre il tradizionale modello in cui il software protegge il software, per stare al passo con le nuove categorie di minacce alla sicurezza (anche digitale) e alla privacy. Combinando la sicurezza olistica con le tecnologie di sicurezza "below-the-OS" (al di sotto del sistema operativo) basate su hardware, è possibile proteggere ogni livello dello stack di elaborazione per prevenire e rilevare gli attacchi alla base, incluse le tipologie di minacce che si verificano più comunemente lungo la supply chain. Il rapporto di collaborazione instauratosi tra Dell, Microsoft e Intel nel campo della progettazione è incentrato sulla copertura della superficie di attacco con un articolato intreccio di tecnologie a livello di componenti e di piattaforma. Oltre ad altri strumenti e tecnologie Dell e Intel, Intel® Hardware Shield e il framework Dell SafeBIOS offrono protezione integrata basata su hardware agli utenti dei dispositivi commerciali Dell.

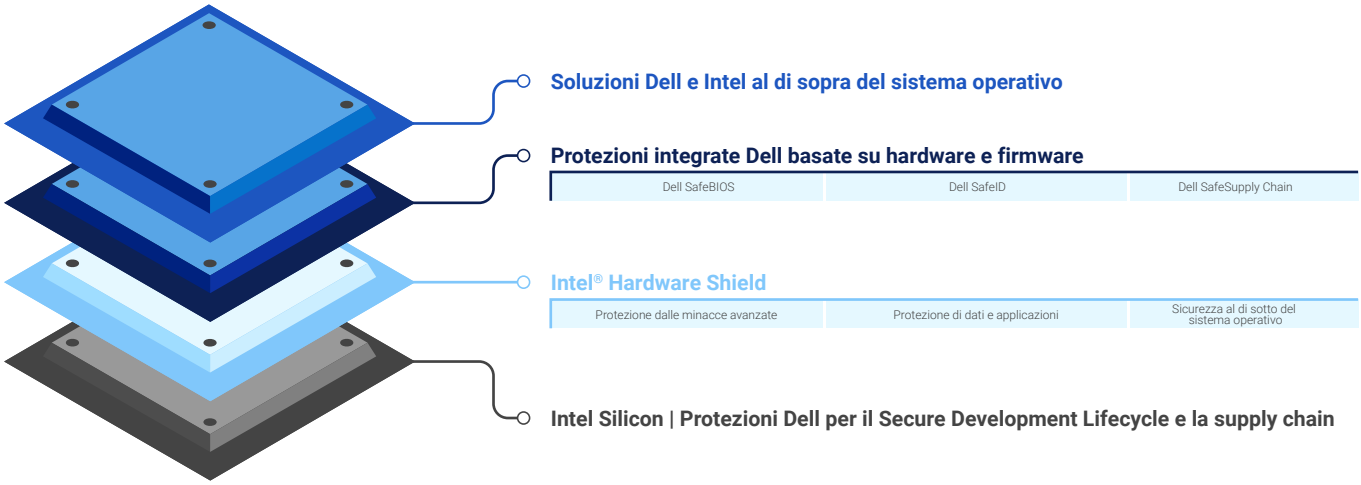


Figura 1: Intel® Hardware Shield e le protezioni Dell basate su hardware formano strati di sicurezza per la difesa dagli attacchi ai livelli di base

Intel® Hardware Shield

Incluso in tutti i dispositivi commerciali Dell dotati di piattaforma Intel vPro®, Intel Hardware Shield offre funzioni di sicurezza potenziate a livello hardware che proteggono tutti i livelli dello stack di elaborazione.

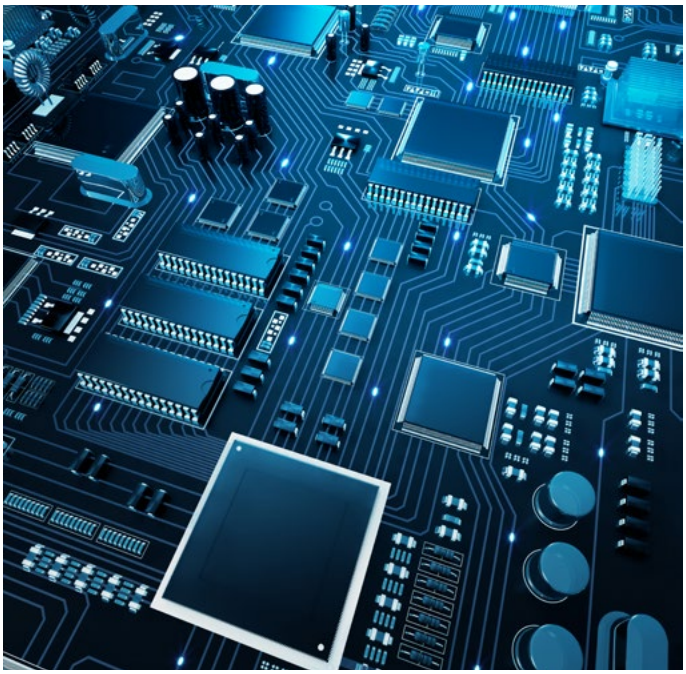
Intel Hardware Shield include protezione contro le minacce avanzate, protezione dei dati e delle applicazioni e sicurezza al di sotto del sistema operativo, contando più di venti tecnologie di sicurezza innovative. Sfruttando quasi tutte queste tecnologie, Dell ha sviluppato soluzioni di sicurezza che attingono dalle relative funzioni di base per fornire ai clienti i dispositivi commerciali tra i più sicuri sul mercato. Queste soluzioni includono il framework Dell SafeBIOS, Dell SafeID e Dell SafeSupply Chain, che insieme forniscono un livello ancora più alto di sicurezza contro le minacce attuali e future.

Tecnologie di sicurezza integrate come mezzo per prevenire, rilevare e contrastare le minacce

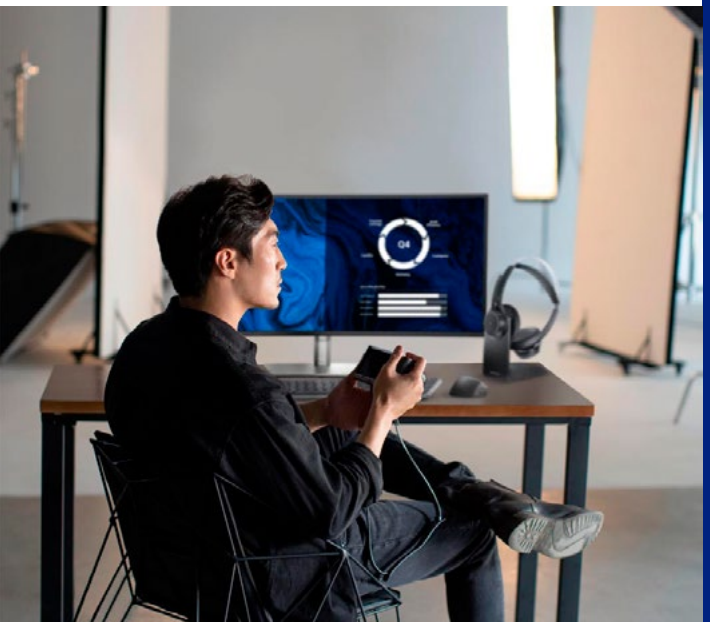
Framework Dell SafeBIOS, Dell SafeID e Dell SafeSupply Chain

Proteggere il BIOS è fondamentale per garantire la sicurezza del dispositivo. Se un malintenzionato riesce a danneggiare il BIOS, sarà in grado di prendere il controllo dell'intero dispositivo in quanto il BIOS si trova in una posizione esclusiva e privilegiata all'interno dell'architettura del dispositivo stesso. Per proteggere questo livello critico, i dispositivi commerciali Dell sono dotati di SafeBIOS, una suite di strumenti che previene gli attacchi al BIOS, rileva se il BIOS è stato compromesso e avvisa l'IT in presenza di eventuali irregolarità.

I dispositivi commerciali Dell selezionati includono anche Dell SafeID, che protegge le credenziali dell'utente finale in un chip di sicurezza dedicato per tenerle al nascosto da malware che cercano e rubano le credenziali di accesso, violazione potenzialmente in grado di compromettere l'intera rete aziendale. Per aumentare ulteriormente la sicurezza dei prodotti, Dell offre funzioni add-on opzionali come Secured Component Verification e gli imballaggi antimanomissione tramite Dell SafeSupply Chain.



Soluzioni Dell e Intel al di sopra del sistema operativo per proteggere gli endpoint



Nonostante la crescente minaccia di attacchi below-the-OS, la protezione al di sopra del sistema operativo è più importante che mai. Con così tanti utenti finali che lavorano da remoto e in viaggio, sono necessarie soluzioni intelligenti che impediscano, rilevino e contrastino le minacce ovunque si verifichino. Dell Trusted Workspace, il nostro portafoglio per la sicurezza degli endpoint, include software opzionali come Dell SafeGuard and Response e Dell SafeData per fornire ai leader aziendali ciò di cui hanno bisogno per proteggere i propri endpoint. Integrate in profondità nel silicio, le funzioni di sicurezza Intel, come la tecnologia Intel® Control-Flow Enforcement, proteggono dagli attacchi rivolti contro il sistema operativo, mentre altre funzionalità all'interno dell'Intel Hardware Shield agiscono al di sotto del sistema operativo preservando dati e applicazioni, oltre a fornire protezione avanzata contro le minacce.

A ciò si aggiunge il livello di sicurezza software di Microsoft, eseguito dalla Security Foundation al cloud. In Windows 11, hardware e software lavorano insieme per proteggere i dati sensibili dal core al cloud. La protezione completa contribuisce a garantire la sicurezza dell'organizzazione, a prescindere da dove i dipendenti lavorino. Nella pagina seguente sono illustrati i livelli di protezione di Windows 11.

Soluzioni Dell, Microsoft e Intel al di sopra del sistema operativo per la protezione degli endpoint

Intel integra ulteriori protezioni hardware a ogni livello della vision di sicurezza di Microsoft. Tali protezioni sono a loro volta integrate nelle soluzioni Dell Client.

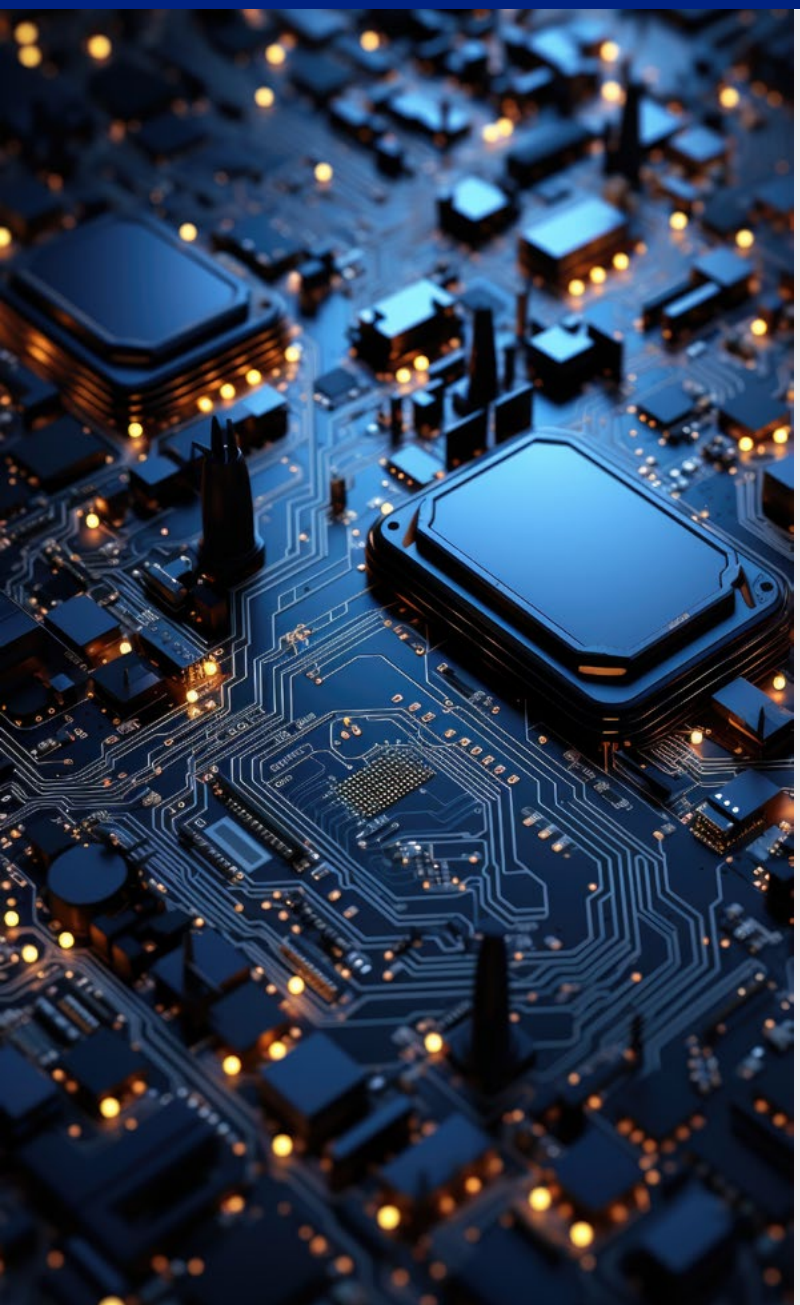
Partnership per fornire protezione efficace di serie.

La sicurezza unica e integrata di Dell Technologies comprende tutte le innovazioni relative alla sicurezza dei nostri partner Intel e Microsoft, così da proteggere la forza lavoro ibrida dalle minacce in continua evoluzione.

Sicurezza di Windows 11

Protezione end-to-end con gestione moderna.

Con funzionalità di protezione pronte all'uso, Windows 11 è il sistema operativo Windows più sicuro di sempre. Hardware e software lavorano insieme per proteggere i dati sensibili dal core al cloud, con strati di protezione a ogni livello dell'hardware, del sistema operativo, delle applicazioni, delle identità e del cloud, il tutto migliorando produttività, sicurezza e resilienza praticamente ovunque.



Hardware (chip)

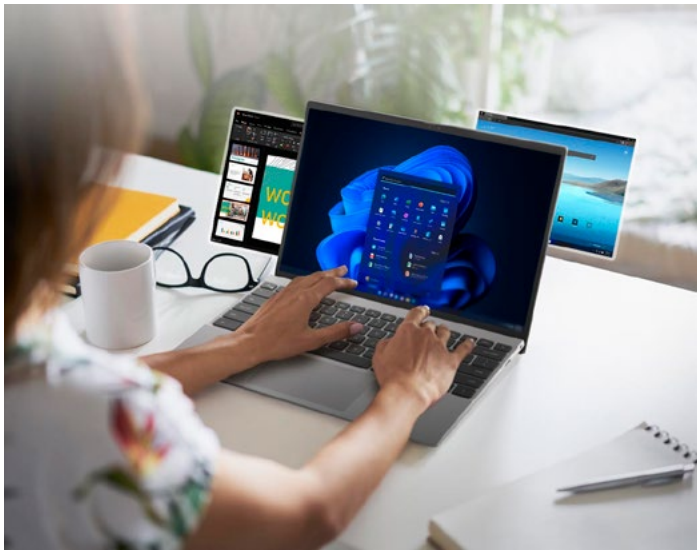
Radice di attendibilità hardware

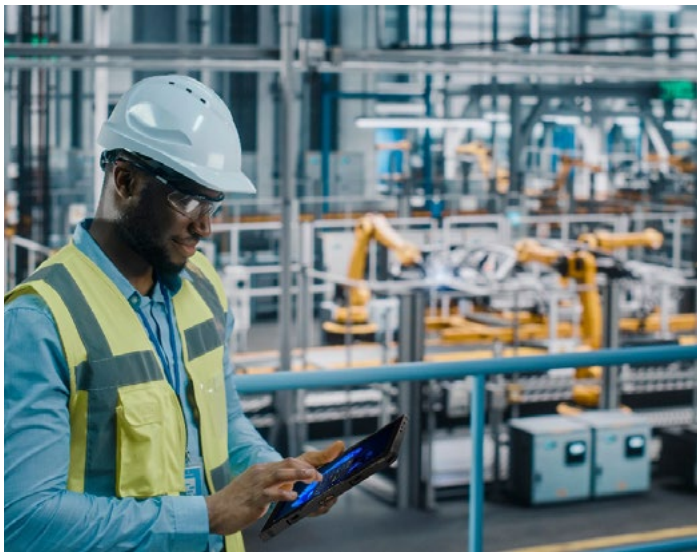
La radice di attendibilità (root of trust) hardware protegge e mantiene l'integrità del sistema durante l'accensione del dispositivo, carica il firmware e avvia il sistema operativo, rispettando importanti obiettivi di sicurezza del sistema.

Trusted Platform Module (TPM)

La tecnologia Trusted Platform Module (TPM) è progettata per fornire funzioni di sicurezza basate su hardware. TPM offre vantaggi a livello di sicurezza e privacy non solo per l'hardware del sistema, ma anche per utenti e proprietari della piattaforma. Windows Hello, BitLocker, System Guard (in precedenza Windows Defender System Guard) e altre funzioni di Windows utilizzano il modulo TPM per funzioni quali la generazione delle chiavi, la protezione dello storage, la crittografia, le misure di integrità all'avvio e l'attestazione.

Sicurezza di Windows 11





Sistema operativo

Sicurezza del sistema

Trusted Boot (Secure Boot + Measured Boot)
Windows 11 richiede che tutti i PC utilizzino la funzione Secure Boot (avvio sicuro) dell'interfaccia UEFI (Unified Extensible Firmware Interface). Quando un dispositivo Windows 11 viene avviato, Secure Boot e Trusted Boot interagiscono tra loro per prevenire attacchi malware ed evitare il caricamento di componenti danneggiati.

Crittografia e protezione dei dati

BitLocker è una funzione di protezione dei dati con crittografia a livello del disco che si integra con il sistema operativo per contrastare minacce quali il furto di dati o l'esposizione ai rischi dovuti a computer persi, rubati o dismessi in modo non appropriato.

Secured-core PC

Microsoft e Dell hanno lavorato insieme per mettere a punto una speciale categoria di dispositivi chiamata Secure-core PC (SCPC). Questi computer sono dotati di ulteriori misure di sicurezza a livello del firmware (o core del dispositivo) a supporto del sistema operativo Windows.

Sicurezza della rete

Per ridurre la superficie di attacco di un'organizzazione, la protezione della rete integrata in Windows evita che gli utenti accedano a domini e indirizzi IP pericolosi che potrebbero ospitare truffe di phishing, exploit e altri contenuti malevoli. Utilizzando servizi basati sulla reputazione, la protezione della rete blocca l'accesso a domini e indirizzi IP con cattiva reputazione potenzialmente dannosi.

Protezione da virus e minacce

Microsoft Defender SmartScreen Microsoft Defender SmartScreen protegge contro phishing, siti web/applicazioni malevoli e download di file potenzialmente dannosi.

Sicurezza di Windows 11

Applicazioni

Smart App Control
Smart App Control evita che gli utenti eseguano applicazioni malevoli sui dispositivi Windows bloccando quelle non affidabili o senza firma. Inoltre, aggiunge un ulteriore layer di sicurezza (oltre alle difese integrate nel browser) inserito direttamente nel core del sistema operativo a livello di processo.

Isolamento delle applicazioni
Disponibile in anteprima pubblica, Win32 è una nuova funzionalità di protezione per l'isolamento delle applicazioni fornita come impostazione predefinita sui client Windows. Questa funzione è basata su AppContainer e offre numerose funzionalità di protezione aggiuntive per consentire alla piattaforma Windows di difendersi dagli attacchi che sfruttano le vulnerabilità nelle applicazioni o nelle librerie di terze parti.

Identità

Accesso senza password
Windows Hello consente agli utenti di accedere senza password utilizzando la biometria o la verifica del PIN, oltre a fornire supporto integrato per lo standard di autenticazione senza password FIDO2. Windows Hello for Business estende le funzioni di Windows Hello per integrarsi con gli account ActiveDirectory e Microsoft Entra ID delle organizzazioni fornendo accesso Single Sign-on alle risorse aziendali o didattiche come OneDrive for Business, programmi di posta elettronica professionali e altre app aziendali.

Protezione avanzata delle credenziali
Oltre all'accesso senza password, le organizzazioni utilizzano Credential Guard e Remote Credential Guard per rafforzare la sicurezza delle credenziali di utenti e domini.

Trasparenza per la privacy e comandi
Nell'area delle notifiche sono presenti icone che mostrano agli utenti le risorse e applicazioni (ad es. microfono e posizione) in uso. Passando sopra l'icona con il cursore del mouse, compare anche una breve descrizione dell'app e della relativa funzione. Le app utilizzano anche le nuove API di Windows per supportare la funzione di disattivazione rapida dell'audio (Quick Mute).

Sicurezza di Windows 11

Cloud

Microsoft Entra ID

Microsoft Entra ID (in precedenza Azure Active Directory) è una soluzione completa e basata su cloud per la gestione delle identità che consente di accedere in modo sicuro ad applicazioni, reti e altre risorse, proteggendole da eventuali minacce.

Microsoft Intune

Microsoft Intune è una soluzione completa per la gestione degli endpoint che consente di proteggere, implementare e gestire utenti, applicazioni e dispositivi. Intune riunisce tecnologie come Microsoft Configuration Manager e Windows Autopilot per semplificare il provisioning, la gestione della configurazione e gli aggiornamenti software all'interno dell'organizzazione.

Servizio di attestazione di Microsoft Azure

Questo servizio verifica da remoto la conformità dei dispositivi alle policy di sicurezza, attestandone il funzionamento affidabile prima che sia loro permesso di accedere alle risorse. Microsoft Intune si integra con il servizio di attestazione di Microsoft Azure per analizzare lo stato dei dispositivi Windows nel complesso e collegare queste informazioni all'accesso condizionale di Microsoft Entra ID.

Dell, Microsoft e Intel investono continuamente nella sicurezza della piattaforma in seguito al rilascio

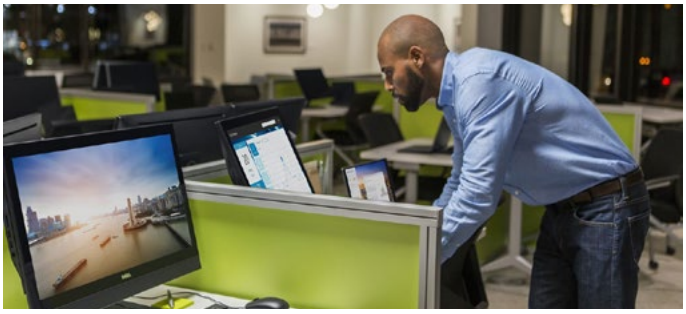
$ 46,4 MLD

Investimenti congiunti in R&S nel 2023*

* Macrotrends.net - Spesa in ricerca e sviluppo nel 2023: Dell Technologies $ 2,88 miliardi, Intel $ 16,046 miliardi e Microsoft $ 27,524 miliardi

Dell, Microsoft e Intel hanno effettuato investimenti significativi e duraturi per garantire la sicurezza durante l'intero ciclo di vita del prodotto. In seguito all'introduzione sul mercato di un dispositivo o di una piattaforma, le tre aziende continuano a testare attivamente i propri prodotti alla ricerca di eventuali vulnerabilità. Per Intel, questo processo include la collaborazione con ricercatori e università al fine di individuare possibili falle di sicurezza prima che lo facciano gli utenti malintenzionati, applicando rapidamente patch per correggere le vulnerabilità rilevate (con relativa segnalazione dopo aver risolto il problema).

Come parte di questo impegno, Intel finanzia uno dei migliori programmi bug bounty del settore, con l'86% delle vulnerabilità rilevate esternamente nel 2021. Le vulnerabilità ed esposizioni comuni (CVE) rilevate tramite questo programma e dai ricercatori interni o esterni vengono registrate in un database pubblico. Come leader nell'ambito del monitoraggio e del reporting delle vulnerabilità post-release, Intel ha registrato e corretto un numero superiore di potenziali vulnerabilità rispetto alla maggior parte dei concorrenti, superando di gran lunga i produttori di chip che non sono allineati a questo impegno a garantire la trasparenza e la sicurezza dei dispositivi.

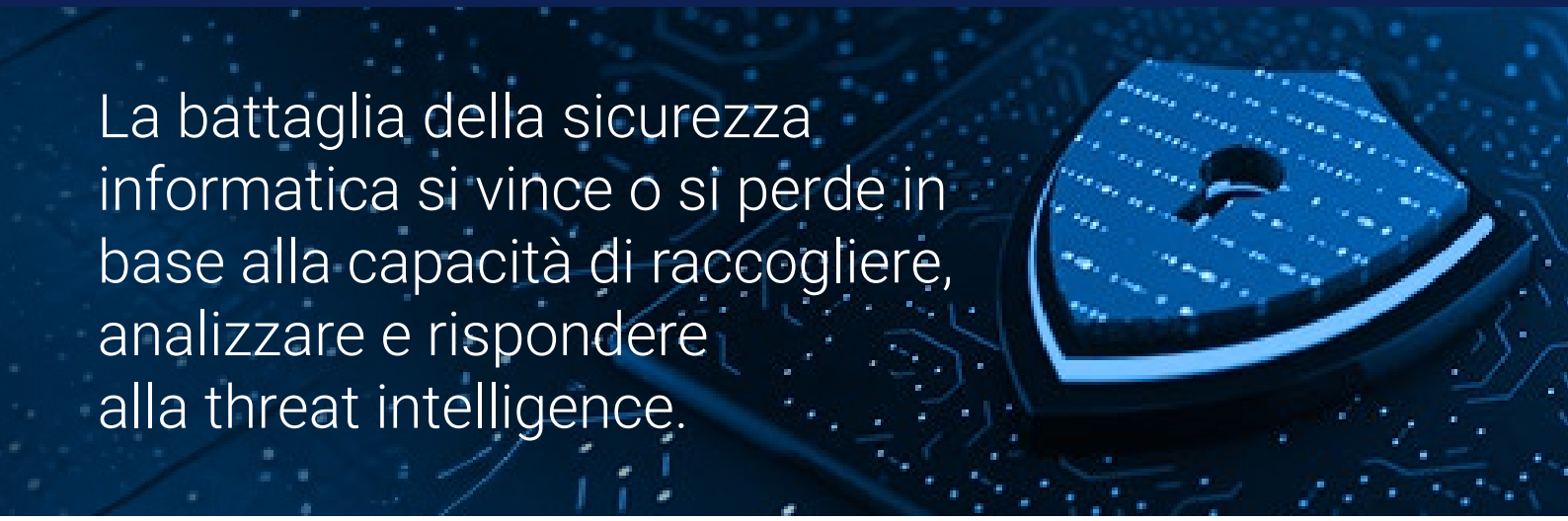


Per risolvere le vulnerabilità e le esposizioni comuni rilevate attraverso i suoi programmi estesi, Intel pubblica regolarmente aggiornamenti della piattaforma per tutti i sistemi in esecuzione sui propri prodotti. Questa implementazione rientra in un processo più ampio che richiede la convalida dall'ecosistema dei partner di Intel, tra cui CSP, ISV, OEM/ODM e SI.

La pubblicazione delle vulnerabilità identificate a livello del prodotto con la relativa risposta è coordinata dai team PSIRT (Product Security Incident Response Team) dedicati di Dell e Intel, i quali lavorano per garantire che le CVE vengano gestite in modo rapido e sicuro, riducendo efficacemente gli eventuali rischi a cui espongono.

Dell, Microsoft e Intel hanno effettuato questi investimenti per fornire supporto costante ai nostri clienti e alleggerire il carico sui propri team IT. Abbiamo assunto ricercatori, security architect e analisti forensi per aiutare i clienti a preservare il proprio business e consentire ai loro team di mettere a disposizione dei dipendenti tutti gli strumenti necessari per svolgere al meglio il proprio lavoro.

L'impegno di Dell, Microsoft e Intel per la crescita del tuo business



La battaglia della sicurezza informatica si vince o si perde in base alla capacità di raccogliere, analizzare e rispondere alla threat intelligence.

I malintenzionati di oggi sono sempre più preparati. Poiché la maggior parte delle soluzioni di sicurezza è progettata per proteggere solo il software, gli hacker sfruttano i livelli al di sotto del sistema operativo e la supply chain come nuovi vettori di attacco per compromettere la sicurezza aziendale e sfruttarne le vulnerabilità.

Per contrastare tali attacchi e proteggere il business, è necessario prendere in considerazione l'uso di tecnologie di sicurezza integrate e basate su hardware quando si installano dispositivi commerciali per i propri dipendenti.

Dell, Microsoft e Intel collaborano da decenni nel campo dei dispositivi commerciali e si sono guadagnate la fiducia dei clienti con alcuni dei dispositivi commerciali più sicuri del settore. La nostra collaborazione a livello progettuale ci permette di rimanere un passo avanti rispetto agli hacker attraverso la nostra coerenza in termini di ricerca, diligenza e innovazione. Come leader nel settore dei dispositivi commerciali da decenni, individuiamo e blocchiamo sempre più minacce, agendo costantemente su data set di grandi dimensioni ed enormi volumi di dati di telemetria per continuare a migliorare la sicurezza dei dispositivi commerciali dei clienti. I nostri leader di pensiero si incontrano regolarmente per discutere di come si configura oggi la sicurezza completa, di come sarà in futuro e di quali investimenti saranno necessari affinché i nostri prodotti siano sempre all'avanguardia per quanto riguarda la sicurezza informatica commerciale.

Con sicurezza della supply chain di massimo livello, protezioni basate su hardware, software per la protezione dalle minacce avanzate e supporto continuo, Dell, Microsoft e Intel offrono alle aziende i dispositivi commerciali di cui hanno bisogno non solo per svolgere il lavoro, ma anche per proteggere i dati aziendali dal dark web. Contatta oggi stesso il responsabile vendite Dell per saperne di più sui nostri programmi per dispositivi commerciali e su come raggiungere gli obiettivi aziendali con la nostra collaborazione.

Clicca qui per conoscere la nostra

strategia completa

DELL Technologies

Windows 11

intel