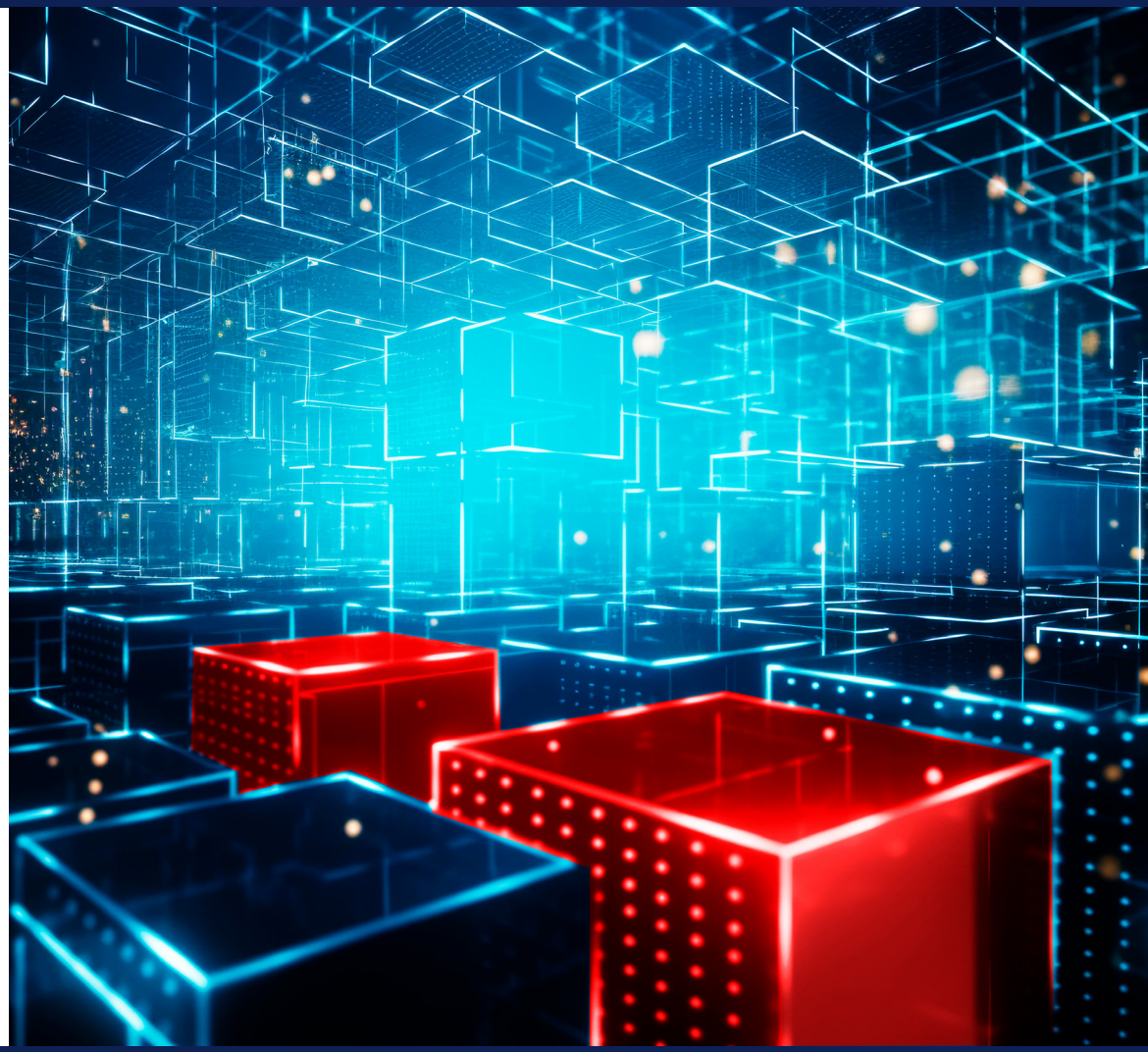
Come proteggere l'utilizzo dell'AI nell'endpoint

Difendete i carichi di lavoro dell'AI on-device con dispositivi sicuri e moderni e una mentalità da malintenzionato.



Executive Summary

L'AI on-device offre enormi vantaggi, ma comporta anche rischi informatici. In questo eBook illustreremo come predisporre la propria organizzazione in modo sicuro per sfruttare l'innovazione dell'AI sull'endpoint.

Sommario

La superficie di attacco dell'AI on-device

Che cosa può essere attaccato

Tutte le tecnologie emergenti presentano un rischio per la sicurezza informatica per un motivo: si tratta di un territorio inesplorato. Si tratta di affrontare l'ignoto. Lo abbiamo visto con cloud computing, blockchain e numerose altre tecnologie. Lo stesso vale per l'AI on-device. La chiave per mitigare questo rischio, come sempre, è gettare luce sull'ignoto.

Prima di poter parlare della sicurezza necessaria per ridurre al minimo la superficie di attacco, è utile parlare di ciò che proteggiamo e del perché. Immaginatelo come un sistema di tubi in un edificio commerciale che ospita più aziende. Questi tubi trasportano acqua, gas e simili in tutta la struttura per vari casi d'uso. Se il materiale che scorre attraverso i tubi è contaminato o interrotto, non può svolgere il proprio lavoro. Se i tubi che trasportano il materiale sono danneggiati o alterati, non possono svolgere il loro lavoro. Sia i tubi sia il loro contenuto devono essere in buone condizioni per soddisfare le esigenze dei rispettivi casi d'uso.►

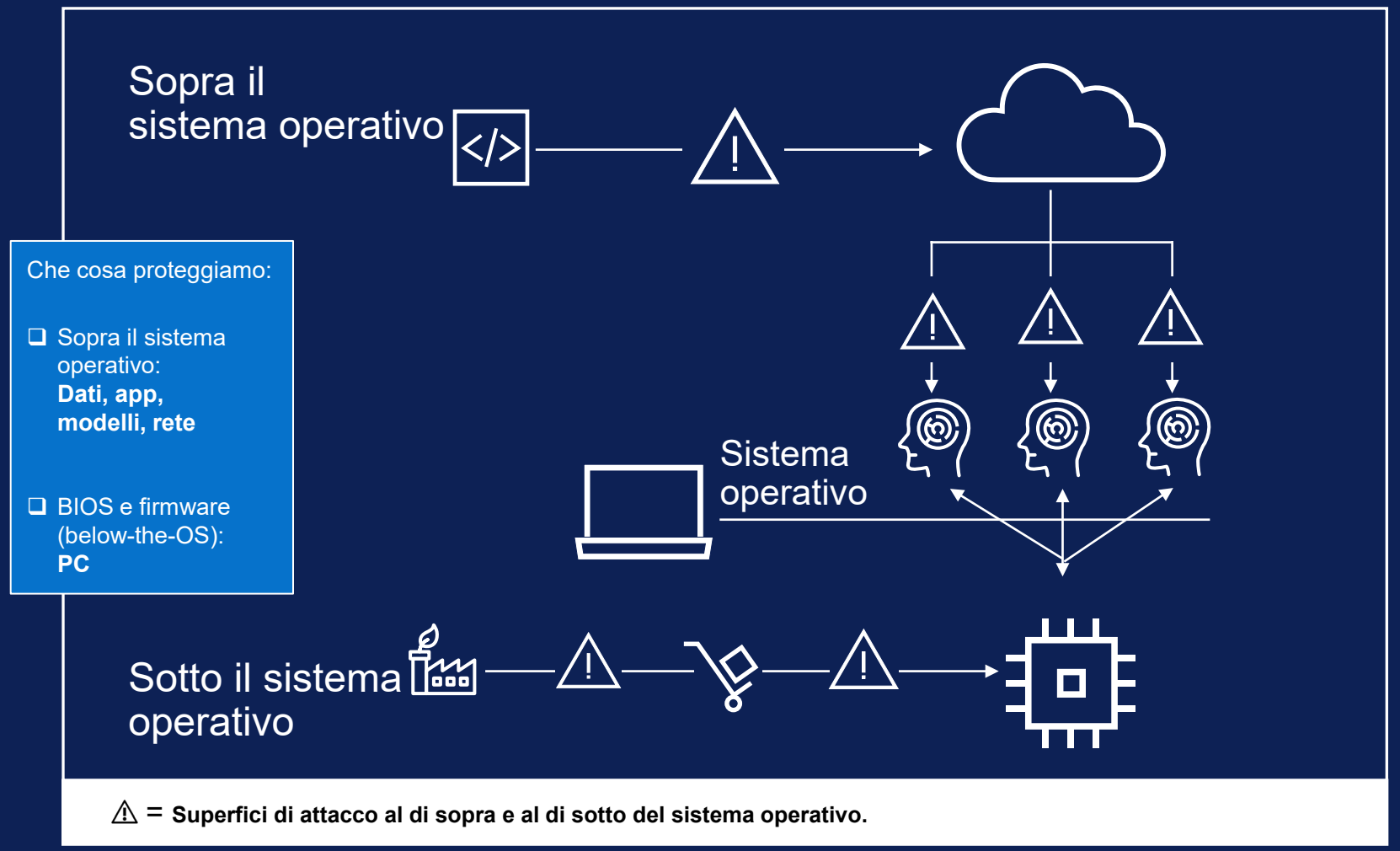
La superficie di attacco dell'AI on-device (continua)

Che cosa può essere attaccato (continua)

Riconducendo l'esempio all'AI sull'endpoint:

- i tubi sono la vostra infrastruttura, ovvero i vostri PC, le vostre reti aziendali. Il modo e il luogo in cui lavorate.
- Il contenuto che passa attraverso i tubi è rappresentato dai dati, dalle app e dai modelli alla base dei vari casi d'uso dell'AI. Gli asset e le risorse di cui avete bisogno per svolgere il vostro lavoro.

E avete indovinato. Gli avversari informatici attaccano entrambi. Possono rubare l'IP per trattenerlo in cambio del pagamento di un riscatto oppure contaminare i dati o i modelli per danneggiare le operazioni. In tutti i casi, le conseguenze possono essere gravi, e portare danni finanziari e reputazionali e/o l'attivazione di controlli normativi.►



Rischi per la sicurezza sull'endpoint

Tattiche utilizzate dagli autori di attacchi per riuscire ad accedere

Ora parleremo dei metodi che gli autori degli attacchi potrebbero utilizzare per riuscire ad accedere a entrambi i loro obiettivi.

Compromissione del dispositivo. Come possiamo vedere in Endpoint Security Market Insights, Forrester Research, Inc. di marzo 2025, i PC sono tra i principali obiettivi delle moderne minacce informatiche. Questo tipo di attacco può verificarsi molto prima che l'AI on-device inizi a lavorare, ad esempio nel caso di un **attacco alla supply chain hardware o software**. Ci sono decine, se non centinaia, di punti lungo la supply chain in cui una parte malintenzionata potrebbe essere in grado di manomettere i componenti, ad esempio circuiti o firmware, per introdurre debolezze che possono essere sfruttate in un secondo momento. Immaginate il disastro incombente per una società di investimenti che riceve una nuova spedizione di PC con componenti contraffatti.

Compromissione dell'identità. Le violazioni che coinvolgono credenziali rubate o compromesse sono uno dei vettori di attacco in più rapida crescita. Non c'è da stupirsi. Gli autori di attacchi informatici che utilizzano credenziali valide possono accedere a un PC, muoversi liberamente all'interno della rete aziendale e passare inosservati per lunghi periodi di tempo. Secondo il più recente report Cost of a Data Breach di IBM, sono stati necessari in media 292 giorni per identificare e contenere tali violazioni, il periodo più lungo di qualsiasi vettore di attacco studiato. Questo livello di accesso è troppo prezioso perché i malintenzionati lo possano ignorare. Infatti, la ricerca di Zscaler mostra che le parti malintenzionate stanno migliorando il furto di credenziali per migliorare e dimensionare gli attacchi di phishing utilizzando l'AI generativa. Questo accesso non autorizzato applicato ai dati sensibili di addestramento o inferenza oppure direttamente ai modelli è classificato come **attacco alla supply chain dei modelli**.

Minaccia interna. Una ricerca recente mostra che, rispetto ad altri vettori di attacco, **gli attacchi malevoli interni** hanno causato i costi più elevati, in media $ 4,99 milioni. Tenete presente che gli attacchi interni possono verificarsi in tutta la supply chain hardware, la supply chain software e la supply chain del modello.▶

Tempo medio necessario a un utente finale per farsi ingannare da un'e-mail di **phishing**: <60 secondi*

292 giorni in media per individuare e contenere **la compromissione delle credenziali****

Gli attacchi malevoli interni costano in media $ 4,99 milioni**

**Fonte: Verizon DBIR, 2024*
***Fonte: IBM Cost of a Data Breach, 2024*

Contromisure da adottare

Che cosa riduce i rischi

Nessuno di questi obiettivi degli attacchi è sostanzialmente nuovo. E nemmeno gli obiettivi finali degli autori degli attacchi. Come sempre, desideriamo concentrarci sul mantenimento della sicurezza e della resilienza della flotta. **Il layering delle contromisure** può contribuire a ridurre la superficie di attacco e gettare subito luce su qualsiasi comportamento sospetto.

Una **mentalità Zero Trust** attenua i rischi in tutta la flotta. Questi principi, ovvero mai fidarsi, verificare sempre e monitorare continuamente, aiutano a essere sempre un passo avanti rispetto agli hacker. È impossibile bloccare il 100% degli attacchi. Per un solido profilo di sicurezza, servono **visibilità e controllo** nell'ecosistema IT.

Tenendo a mente questo quadro, rivalutate la vostra infrastruttura, in particolare i sistemi e i processi che interagiscono con l'AI. Quali contromisure riducono al minimo il rischio di compromissione dei dispositivi, di compromissione dell'identità e di minacce interne?►

I principi Zero Trust offrono protezione dai rischi e riducono il raggio d'azione dell'attività informatica

Contromisure da adottare (continua)

Che cosa riduce i rischi (continua)

Esistono due categorie di contromisure generali.

La sicurezza "al di sotto del sistema operativo" protegge i dispositivi AI su cui lavorate. Possiamo suddividere questo aspetto in due parti:

- Difendete la vostra flotta con dispositivi **creati in modo sicuro**. Ciò significa utilizzare AI PC sicuri fin dalla progettazione, ovvero sviluppati con principi di progettazione sicuri e in una supply chain sicura.
- Difendete la vostra flotta con dispositivi dotati **di sicurezza integrata**. Gli AI PC sicuri includono livelli di protezione integrata che offrono visibilità, fino ai livelli di BIOS e silicio, fin dal primo utilizzo.

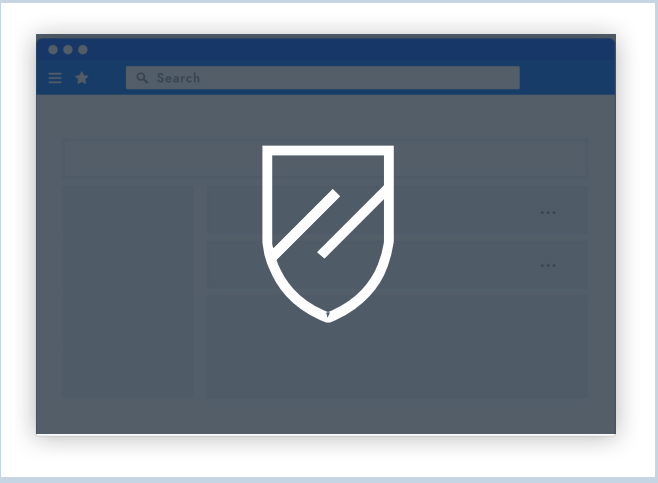
La sicurezza "al di sopra del sistema operativo" protegge l'accesso ai modelli di AI. Difendete i dati e i modelli *con* cui lavorate e le reti aziendali *in* cui lavorate con la **sicurezza software**. È essenziale proteggere le operazioni di sicurezza dell'apprendimento automatico e monitorare il traffico di rete dei carichi di lavoro di AI implementati.►

Sicurezza al di sotto del sistema operativo

PC AI sicuri

Sicurezza hardware e firmware, sicurezza della supply chain, componenti elettronici

Sicurezza al di sopra del sistema operativo



Sicurezza software

Ulteriore livello di sicurezza per endpoint, reti e ambienti cloud

Servizi di sicurezza e competenze disponibili per unire insieme il tutto.

Applicazione delle best practice alla flotta

In che modo gli AI PC Dell offrono sicurezza di base per la vostra flotta

È qui che Dell Trusted Workspace può aiutarvi. I nostri tecnici elaborano e progettano la sicurezza dei nostri AI PC commerciali con una profonda comprensione della mentalità da malintenzionato.

Al di sotto del sistema operativo, la progettazione mirata alla sicurezza, i rigorosi controlli della supply chain e la garanzia della supply chain opzionale aiutano a garantire che i PC siano sicuri fin dal primo avvio. La sicurezza integrata a livello hardware e firmware mantiene il PC protetto durante l'utilizzo, ad esempio con il rilevamento dei tentativi di manomissione a livello di BIOS (Dell SafeBIOS) e la sicurezza delle credenziali senza password (Dell SafeID) esclusivi di Dell per proteggerlo da accessi non autorizzati. Inoltre, le tecnologie a livello di silicio di Intel® offrono una base per proteggere vari aspetti dell'AI quando viene utilizzata dai clienti degli AI PC. Ad esempio, Intel aiuta a proteggere i dati dell'AI inattivi sul client con l'accelerazione per la crittografia dei modelli su disco.►

Applicazione delle best practice alla flotta (continua)

In che modo gli AI PC Dell contribuiscono a offrire sicurezza di base per la vostra flotta (continua)

Per integrare questa sicurezza al di sotto del sistema operativo, la tecnologia Persistence del nostro partner Absolute può essere integrata in fabbrica per una visibilità e un controllo ancora maggiori nell'intero ciclo di vita del PC, rendendo possibili, ad esempio, la geolocalizzazione dei dispositivi lungo il percorso e il self-healing delle app critiche nello scenario peggiore.

Infatti, Dell ha curato un ecosistema di soluzioni dei partner software, tra cui CrowdStrike Falcon XDR e Absolute Secure Access, che attivano i principi Zero Trust per proteggere la supply chain del modello da accessi non autorizzati **al di sopra del sistema operativo**. Utilizzando queste soluzioni, è possibile creare e applicare policy con controlli granulari degli accessi (ad esempio, controllo degli accessi basato sui ruoli o RBAC) per ridurre il rischio che utenti interni malintenzionati accedano o manipolino i modelli di AI.►

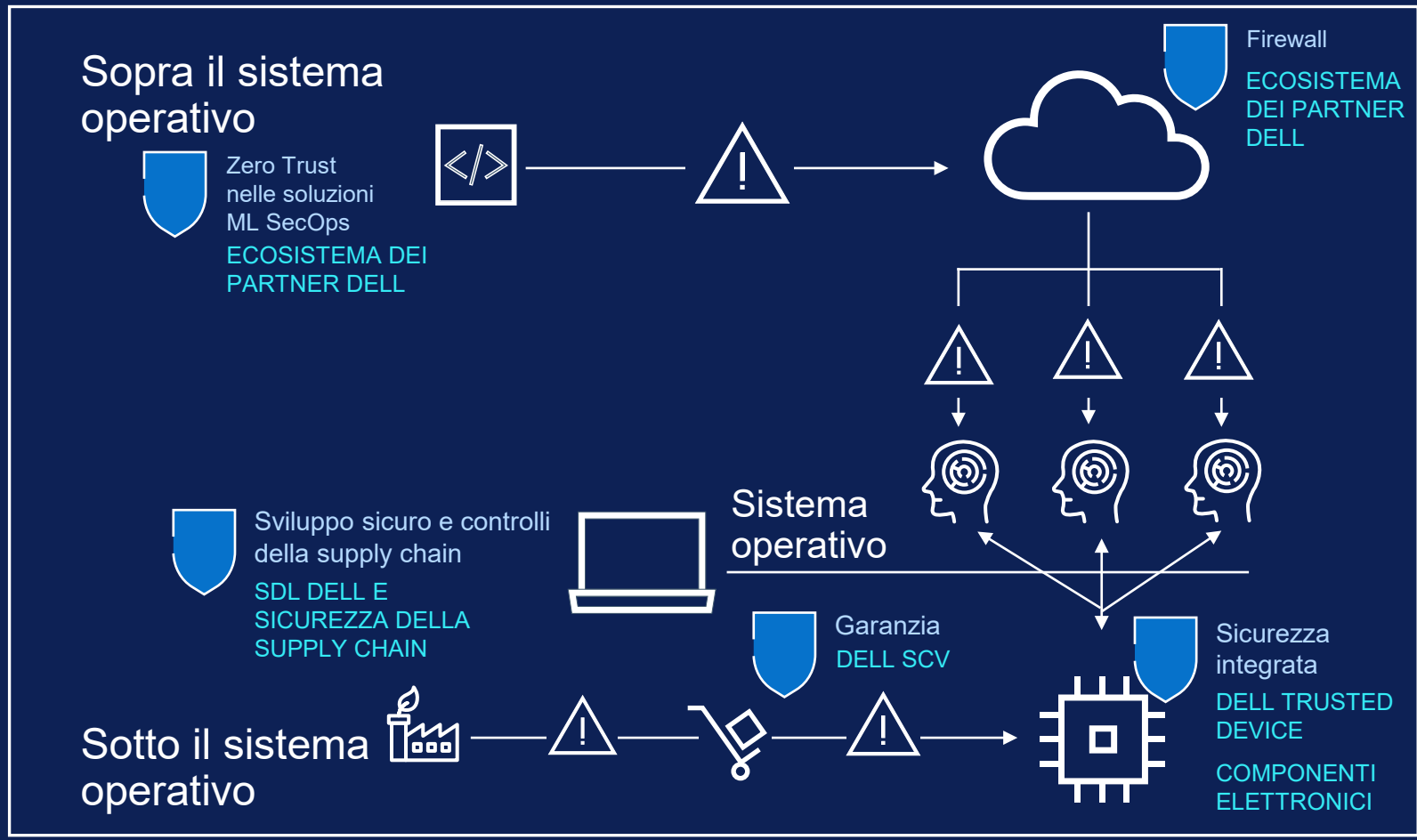
Applicazione delle best practice alla flotta (continua)

In che modo gli AI PC Dell contribuiscono a offrire sicurezza di base per la vostra flotta (continua)

Insieme, tutto ciò costituisce la ***sicurezza per l'AI***. Queste funzionalità difendono i carichi di lavoro dell'AI on-device dagli attacchi informatici, per rimanere concentrati sull'innovazione e sul consolidamento del business.►

Bloccate gli attacchi avanzati agli endpoint con difese hardware e software coordinate

Dell collabora con Intel e CrowdStrike per integrare i livelli al di sotto e al di sopra del sistema operativo con la sicurezza assistita da hardware.
Ulteriori informazioni >



Considerazioni principali e passaggi successivi

Protezione dell'AI sull'endpoint con Dell

Le aziende sono entusiaste dell'AI, ma secondo un recente sondaggio condotto da Absolute sui CISO, l'idoneità all'AI è in ritardo. Un'analisi effettuata su milioni di dispositivi ha rivelato che il popolamento dei PC non è in grado di assorbire ampiamente le nuove funzionalità dell'AI. **Dell è in grado di riunire tutto in un'unica soluzione.**

Sviluppo e implementazione dei modelli di AI su una base sicura e moderna. Il supporto per Windows 10 termina nel mese di ottobre 2025. I PC non riceveranno più aggiornamenti di sicurezza, aggiornamenti delle funzionalità e supporto per Windows 10. È possibile che i dispositivi più obsoleti non soddisfino i requisiti di Windows 11 e non dispongano dei miglioramenti più recenti integrati a livello di prestazioni, sicurezza e AI. Passate a **Dell Pro** o **Dell Pro Max basato su processori Intel® Core™ Ultra con Intel vPro®** per sbloccare i vantaggi in termini di sicurezza e difendere i carichi di lavoro AI con gli **AI PC commerciali più sicuri al mondo.*** ►

Il supporto per Windows 10 termina a ottobre.

Eseguite l'aggiornamento agli AI PC Dell più recenti su Intel per sbloccare i vantaggi in termini di sicurezza e i miglioramenti a ivello di AI:

Acquista Dell Pro ● Dell Pro Max

*Gli AI PC commerciali più sicuri al mondo**

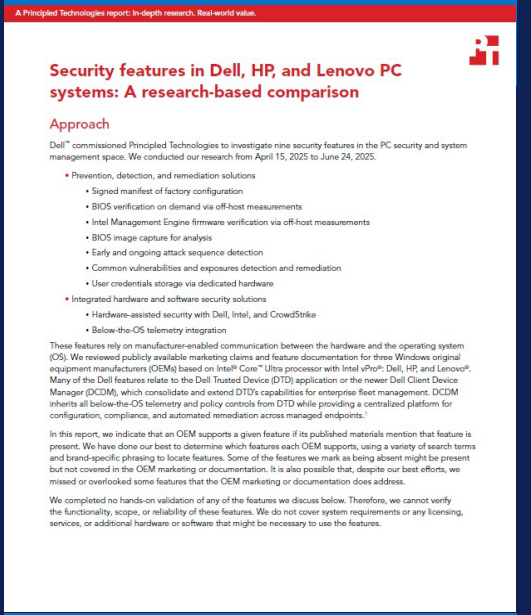
Scoprite software e servizi a valore aggiunto per migliorare il vostro profilo di sicurezza:

Software e integrazioni

Servizi

LEADERSHIP NEL SETTORE

Principled Technologies ha rilevato che la sicurezza a livello degli AI PC commerciali di Dell e Intel è vincente rispetto a quella dei suoi concorrenti


A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Leggi lo studio

Declinazioni di responsabilità

Dati basati su analisi di terze parti di Principled Technologies confrontando gli AI PC commerciali Dell su processori Intel rispetto a HP e Lenovo, luglio 2025. Dati supportati da analisi interne Dell sul mercato mondiale dei PC, ottobre 2024. Applicabile ai PC su processori Intel. Non tutte le funzionalità sono disponibili per tutti i PC. Sono necessari ulteriori acquisti per alcune funzionalità.

Per saperne di più:

Contattaci: Global.Security.Sales@Dell.com

Visita: Dell.com/Endpoint-Security

Seguici: LinkedIn @DellTechnologies | X @DellTech

Informazioni su Dell Endpoint Security

Quello della sicurezza è un argomento che incute timore alle organizzazioni di tutte le dimensioni. **Coinvolgete un partner di grande esperienza nel campo della protezione e della tecnologia per modernizzare la sicurezza degli endpoint**.

Dell Trusted Workspace aiuta a proteggere gli endpoint per un ambiente IT moderno e pronto per Zero Trust. Riducete la superficie di attacco e migliorate la cyber-resilienza con un portafoglio completo di protezioni hardware e software esclusive Dell. Il nostro approccio altamente coordinato e basato sulla difesa contrasta le minacce grazie a una combinazione di protezioni integrate e vigilanza costante. Gli utenti finali rimangono produttivi e l'IT si sente al sicuro grazie alle soluzioni di sicurezza pensate per il mondo di oggi basato sul cloud.