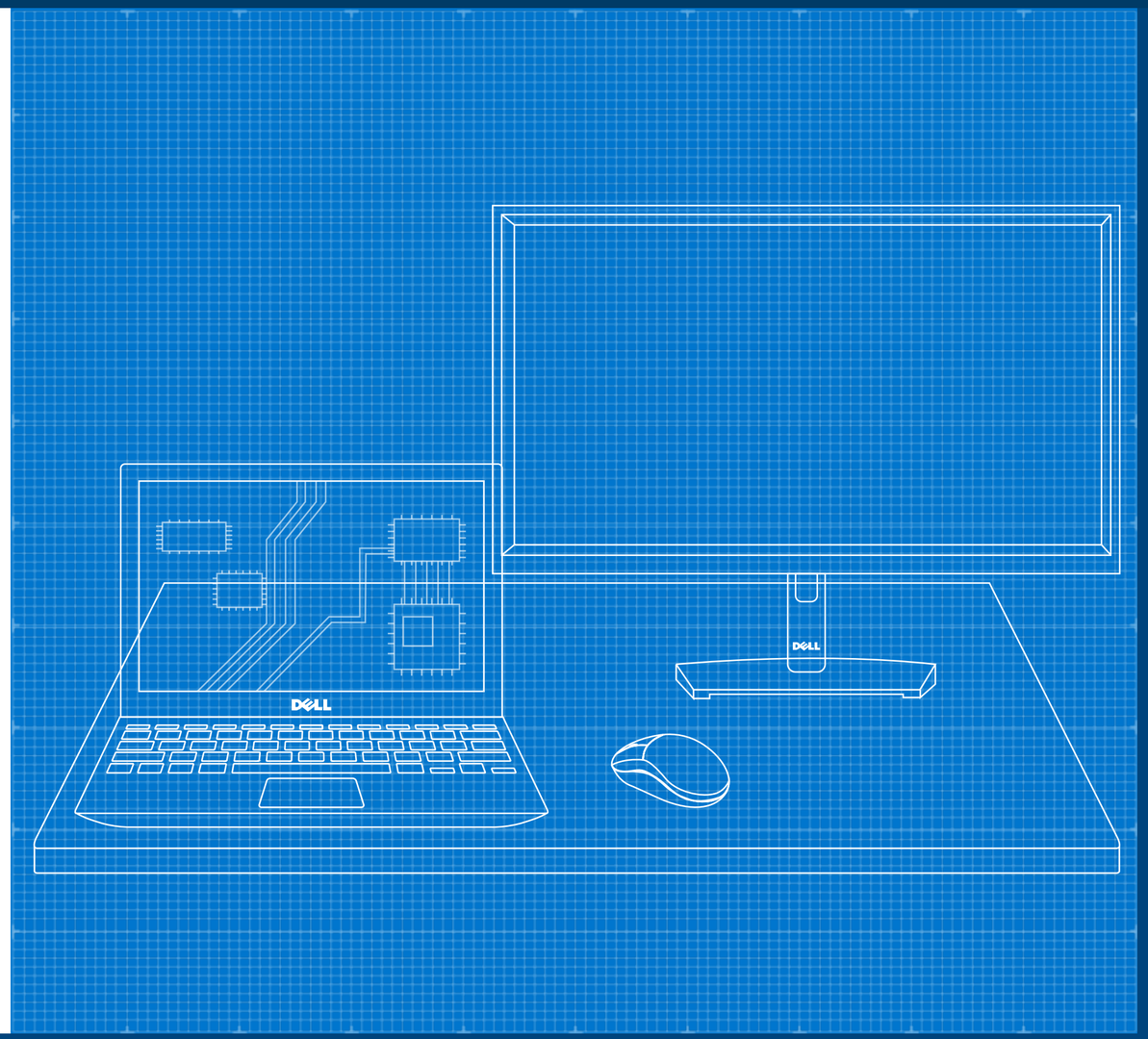
DELL Technologies

# Anatomia di un ambiente di lavoro affidabile

## Migliora la sicurezza della tua flotta con più livelli di difesa



# Executive Summary

Gli attacchi informatici, sempre più numerosi e sofisticati, sono inevitabili. I dispositivi endpoint, le reti e gli ambienti cloud sono diventati i principali bersagli.

Questo eBook offre ai responsabili delle decisioni IT e della sicurezza indicazioni sugli elementi necessari per difendere nel modo più efficace possibile gli endpoint e contrastare questo panorama di minacce in continua evoluzione.

# Sommario

# Il panorama delle minacce

Il passaggio al lavoro ibrido ha introdotto nuove complessità e vettori di attacco e **gli endpoint, le reti e i cloud stanno espandendo le superfici di attacco.**

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*.

Per contrastare queste minacce, molte organizzazioni hanno intrapreso un percorso verso la sicurezza Zero Trust. Tuttavia, per attivare i principi Zero Trust, è necessario garantire l'affidabilità dei dispositivi.

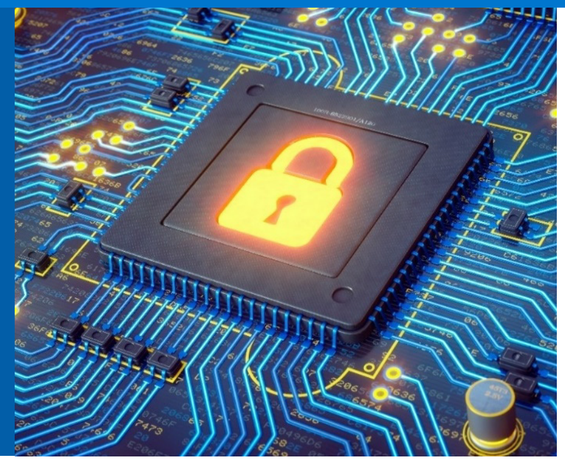
**Come si garantisce l'affidabilità dei dispositivi** ora che gli attacchi stanno diventando più frequenti e la tecnologia avanzata sta creando nuovi vettori di attacco?

[1]CrowdStrike Global Threat Report, 2024.

[2] Dell Innovation Index, 2023.

## Forse non tutti sanno che...

Il 75% degli attacchi nel 2023 non era basato sul malware[1]



Solo il 41% delle organizzazioni intervistate può affermare con assoluta certezza che la sicurezza è parte integrante delle proprie tecnologie e applicazioni[2]

**Stai valutando l'approccio Zero Trust per migliorare la maturità della tua sicurezza informatica?** Leggi il nostro eBook: *La sicurezza degli endpoint è fondamentale per il percorso Zero Trust*.

# Sfide

## Per una sicurezza degli endpoint efficace, è importante capire l'avversario e come opera.

Considerando il potenziale profitto di una violazione, **gli hacker spesso provano più volte a infiltrarsi nella stessa organizzazione, sfruttando metodi e punti di ingresso differenti per incrementare le loro possibilità di successo.** Ad esempio, durante il ciclo di vita di un singolo dispositivo, gli hacker possono tentare di sfruttarne le vulnerabilità attraverso decine di vettori.

**Le difese legacy non sono sufficienti per garantire la sicurezza degli endpoint.** Quando le organizzazioni consolidano una superficie di attacco, gli autori delle minacce si spostano semplicemente su bersagli più esposti. Il passaggio all'ibrido in tutto il mondo ha consentito agli autori delle minacce di identificare nuovi vettori di attacco per gli endpoint che hanno prodotto conseguenze devastanti.

Sulla destra sono riportati alcuni esempi di attacchi

**Attacco alla supply chain: diretto ai fornitori** per ottenere l'accesso ai loro sistemi, ai dati e/o alla rete e, di conseguenza, a quelli dei loro clienti. **Ad esempio, un attacco alla supply chain hardware avviato tramite la manomissione di un componente:**

Gli hacker intercettano una spedizione di PC e sostituiscono i dischi rigidi.

L'IT implementa i dispositivi compromessi nell'azienda.

L'hacker installa un malware per estrarre le credenziali quando gli utenti accedono ai PC.

**Attacco di social engineering: induce gli utenti finali** a fornire informazioni sensibili che possono essere usate per ottenere l'accesso ai dispositivi e alla rete. **Ad esempio, un attacco di spoofing avviato da un'e-mail di phishing:**

L'utente finale viene ingannato da un'e-mail di phishing e fornisce le credenziali a una pagina web falsificata tramite spoofing.

L'hacker usa credenziali valide per accedere in remoto alla rete.

L'hacker esfiltra i dati su un servizio web, crittografa i dati sottratti e li trattiene al fine di chiedere un riscatto.

# Protezione dell'ambiente di lavoro moderno

**Quando si parla di protezione degli endpoint, è necessario un approccio basato da un lato su prevenzione, rilevamento e risposta e dall'altro su ripristino e correzione, da implementare nei vari stati dell'intero ciclo di vita di un dispositivo,** dall'approvvigionamento alla produzione dei PC, dalla spedizione al deployment e dall'utilizzo al ritiro. Immagina quanto può essere ampia una superficie di attacco che combina tutti questi aspetti.

**La strategia più efficace di sicurezza informatica prevede la pianificazione di contromisure per lo scenario peggiore.** Presuppone la possibilità di una violazione e integra diversi livelli di protezione per bloccare l'attacco con la maggiore tempestività e frequenza possibile. Include anche capacità di correzione per ridurre al minimo il rischio di reiterazione.

[3] Dell Innovation Index, 2023.

**PREVENZIONE**

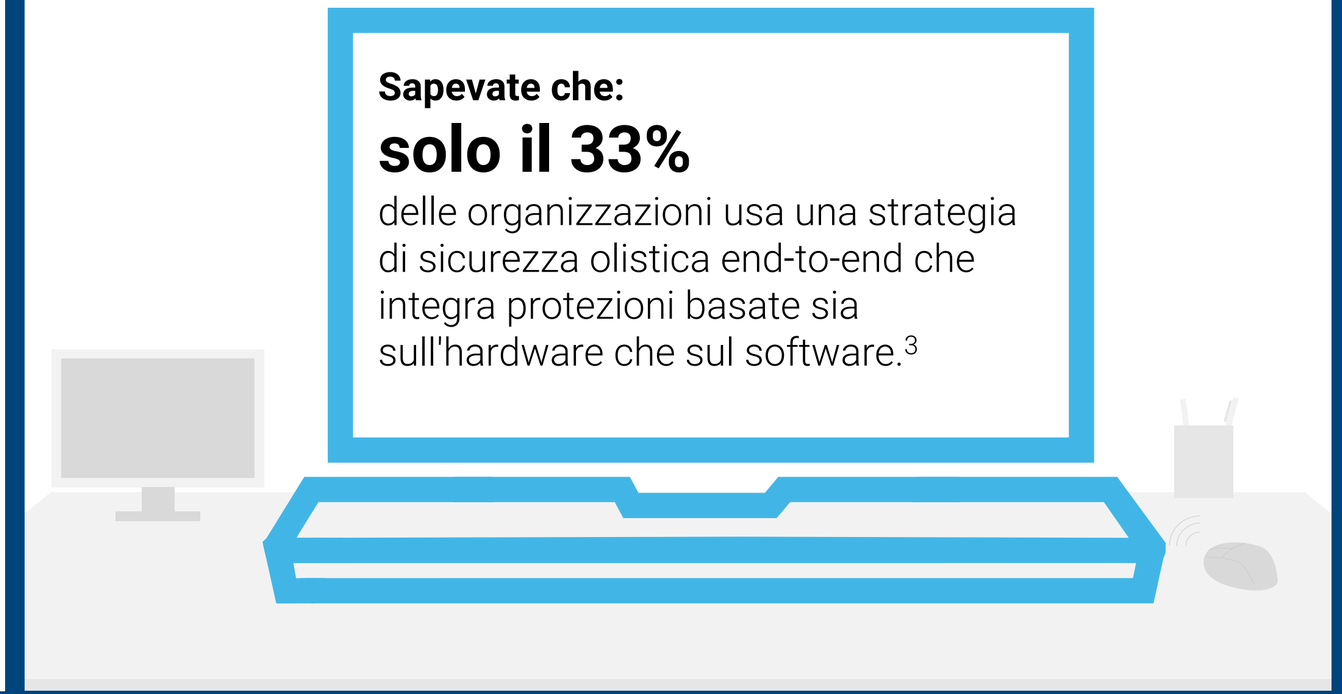
*Riduci le vulnerabilità grazie a misure di difesa progettate per bloccare gli attacchi.*

**RILEVAMENTO E RISPOSTA**

*Contempla sempre la possibilità di una violazione e resta all'erta.*

**RIPRISTINO E CORREZIONE**

*Mitiga l'impatto di un attacco e torna normalmente al lavoro.*



# Anatomia di un ambiente di lavoro affidabile

La sicurezza degli endpoint moderna richiede tre elementi:

1. **Sicurezza software:** oggi più che mai, utenti, dispositivi e dati si trovano spesso al di fuori delle reti aziendali. La sicurezza software non protegge solo i dispositivi, ma estende la protezione agli ambienti di rete e cloud, dove spesso hanno origine le attività malevole.

2. **Sicurezza hardware:** i dispositivi devono integrare funzionalità di protezione. Questo aspetto riguarda la sicurezza hardware e firmware, che protegge il dispositivo durante l'utilizzo. Per difendere l'ambiente di lavoro, è necessaria una funzionalità integrata che offra visibilità e controllo sul dispositivo.

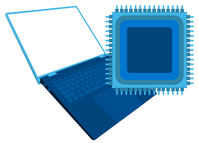
3. **Sicurezza della supply chain:** i dispositivi devono essere realizzati in modo sicuro. Questo significa collaborare con fornitori che a) comprendono il panorama delle minacce e b) sono in grado di usare le loro conoscenze per rispondere all'evoluzione delle minacce. Progettare, sviluppare e testare i PC in modo sicuro riduce il rischio di vulnerabilità nei prodotti, mentre i controlli della supply chain mitigano il rischio di manomissione dei prodotti.

## Analisi dei diversi livelli di sicurezza

*(Esempi illustrativi delle misure di sicurezza elencate)*

### Sicurezza software

- Antivirus di nuova generazione (NGAV)
- Rilevamento e risposta degli endpoint (EDR)
- Rilevamento e risposta estesi (XDR)
- Protezione dei dati su cloud
- Protezione della rete
- Self-healing automatizzato



### Sicurezza hardware e firmware

- Verifica all'avvio
- Verifica al runtime
- Autenticazione degli utenti
- Notifiche di sicurezza e avvisi/telemetria

### Sicurezza della supply chain

- Procedure di sviluppo protette
- Procedure della supply chain protette
- Verifica dei componenti
- Packaging a prova di manomissione

# Il nostro approccio: Dell Trusted Workspace

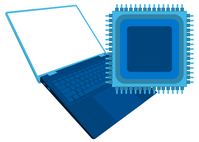
Dell è partner di organizzazioni di tutto il mondo negli ambiti dell'IT e della sicurezza. A differenza delle soluzioni mirate, Dell si concentra sui risultati di sicurezza complessivi grazie a una suite di soluzioni in grado di interrompere le kill chain e aumentare la resilienza dei sistemi agli attacchi informatici. **Dell Trusted Workspace include:**

- Esclusive **protezioni hardware e firmware** che rendono i PC commerciali Dell i più sicuri al mondo.[4] *(Sicurezza con componenti aggiuntivi e integrata)*
- La collaborazione con un ecosistema di partner che sviluppano **software leader del settore** offre una protezione dalle minacce avanzata per il dispositivo, che si estende anche alla rete e al cloud. *(Sicurezza integrata)*

[4]Dati basati su analisi interne Dell, ottobre 2024. Applicabile ai PC su processori Intel. Non tutte le funzionalità sono disponibili con tutti i PC. Per alcune funzionalità è necessario un acquisto aggiuntivo. Convalidato da Principled Technologies. A comparison of security features, aprile 2024.

### Sicurezza software con soluzioni *offerte* dall'ecosistema dei partner

- **Dell SafeGuard and Response: CrowdStrike** e **Secureworks** forniscono soluzioni di rilevamento delle minacce, risposta e correzione.
- **Dell SafeData: Netskope** offre visibilità, monitoraggio e prevenzione della perdita di dati per le app basate su cloud. **Absolute** abilita funzionalità di self-healing per app e reti.



### Sicurezza hardware e firmware integrata nei PC commerciali più sicuri al mondo[4]

*Esempio di funzionalità che proteggono il dispositivo in uso:*

- Le funzionalità off-host di **Dell SafeBIOS,** BIOS Verification*, Indicatori di attacco* e Rilevamento CVE, consentono di rilevare le attività malevole prima che compromettano il PC.
- **Dell SafeID** protegge le credenziali utente in un chip di sicurezza.*
- La funzionalità **Off-host Firmware Verification** protegge l'integrità del firmware con privilegi elevati.*
- Nell'**app Dell Trusted Device**, Dell integra la telemetria del dispositivo con software leader del settore per ottimizzare la sicurezza dell'intera flotta.*

### Sicurezza della supply chain con componenti *aggiuntivi* che garantisce la protezione dei PC fin dal primo avvio

- I componenti aggiuntivi di **Dell SafeSupply Chain**, come la funzionalità Dell Secured Component Verification* (SCV), offrono un'ulteriore garanzia per l'integrità dei prodotti.

** Esclusiva Dell*

# Integrazione di tutti gli elementi con Dell

Adottando le adeguate contromisure, sia hardware che software, puoi ridurre la superficie di attacco e implementare difese che contribuiscono a bloccare gli attacchi comuni.

Le capacità di rilevamento e risposta si concentrano sugli attacchi più infidi che potrebbero passare inosservati.

**Nel caso dell'attacco alla supply chain discusso a pagina 4,** quando si lavora con Dell, l'adozione di misure preventive come le **procedure della supply chain protette** possono bloccare tempestivamente un attacco nella kill chain. Se un attacco riesce a superare queste procedure, si applicano ulteriori contromisure, come la **Verifica dei componenti protetti (SCV)**.

**Nel caso dell'attacco di social engineering**, anche se un hacker riesce a ingannare un utente e a sottrarre le sue credenziali valide, **una verifica utente basata su hardware come SafeID** può bloccare l'attacco tempestivamente e rifiutare ulteriori accessi. Un software per la sicurezza come **Next-Gen Secure Web Gateway** può fornire un altro livello di protezione tramite monitoraggio.

## Come bloccare un attacco alla supply chain hardware avviato tramite la manomissione di un componente.

Gli hacker intercettano una spedizione di PC e sostituiscono i dischi rigidi.

- **Procedure della supply chain protette**
- Packaging a prova di manomissione
- Serrature

*L'IT implementa i dispositivi compromessi nell'azienda.*

- Secured Component Verification (SCV)
- Verifica al runtime

*L'hacker installa un malware per estrarre le credenziali quando gli utenti accedono ai PC.*

- Cloud Access Security Broker
- Next-Gen Secure Web Gateway

## Come bloccare un attacco di social engineering avviato da un'e-mail di phishing.

L'utente finale viene ingannato da un'e-mail di phishing e fornisce le credenziali a una pagina web falsificata tramite spoofing.

- NGAV
- EDR
- XDR

L'hacker usa credenziali valide per accedere in remoto alla rete.

- **Autenticazione a più fattori con SafeID**
- Accesso alla rete Zero Trust

*L'hacker esfiltra i dati su un servizio web, crittografa i dati sottratti e li trattiene al fine di chiedere un riscatto.*

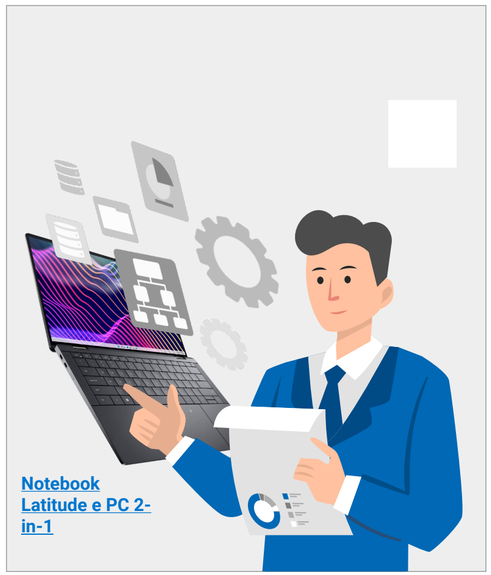
- Next-Gen Secure Web Gateway + Analisi del comportamento degli utenti e delle entità

# Messaggi principali

**Le violazioni sono inevitabili.** Una strategia per la sicurezza degli endpoint efficace prevede sempre lo scenario peggiore e si concentra sull'interruzione delle kill chain ovunque si verifichino, dal dispositivo, alla rete, al cloud.

**Nessuna soluzione blocca il 100% degli attacchi.** È opportuno combinare le contromisure hardware e software per mettere in campo la miglior difesa possibile.

**Il livello della tua sicurezza dipende strettamente da quello dei tuoi fornitori.** Chiedi ai tuoi fornitori di delineare le loro misure di sicurezza.



Notebook Latitude e PC 2-in-1

**Per saperne di più:**

**Contattaci:** Global.Security.Sales@Dell.com

**Visita:** Dell.com/Endpoint-Security

**Seguiteci: LinkedIn** @DellTechnologies | X @DellTech

# Passa alla fase successiva

Quello della sicurezza è un argomento che incute timore alle organizzazioni di tutte le dimensioni. **Coinvolgi 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. Riduci la superficie di attacco 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.