La sicurezza degli endpoint è fondamentale per il percorso verso la Zero Trust

Tre consigli per preparare la strategia Zero Trust

DELL Technologies

Executive Summary

Zero Trust è un percorso a lungo termine. Non è un prodotto o una soluzione da implementare, ma un framework strategico che le organizzazioni costruiscono nel tempo per gestire la sicurezza. Questo eBook contiene indicazioni pratiche per i responsabili delle decisioni IT che si trovano ad affrontare la trasformazione Zero Trust e si concentra, in particolar modo, sul ruolo della sicurezza dei dispositivi endpoint nella costruzione di fondamenta moderne e davvero sicure per il mondo di oggi nel quale si lavora praticamente ovunque.

Sommario

Stato informatico dell'unione

Le minacce alla sicurezza sono in aumento in questo mondo del lavoro sempre più remoto/ibrido e basato sul cloud.

Negli ultimi anni si è registrato un radicale aumento della complessità della protezione dei data asset delle organizzazioni. Il cloud è stato rivoluzionario per la produttività aziendale con la diffusione del lavoro da remoto/ibrido, ma comporta anche dei costi. La transizione dalla sola gestione dell'infrastruttura on-premise all'inclusione del cloud ha ampliato la superficie di attacco per gli avversari e le relative conseguenze. Ad esempio, se un utente malintenzionato riesce nel suo scopo, è possibile che le sue azioni vadano a colpire ogni cliente del servizio cloud in questione, nonché i loro clienti nell'intera supply chain. I potenziali vantaggi per i malintenzionati, che siano stati nazionali o criminali comuni, sono enormi e aprono la strada a nuove vulnerabilità da sfruttare.

Si prevede che il costo per i danni causati dal crimine informatico nel mondo raggiunga **$ 10,5 bilioni entro il 2025**[i]

Nel suo studio 2022, Verizon ha segnalato **5.200** violazioni dei dati confermate, **1,3 volte quelle riscontrate l'anno precedente**[ii]

Implicazioni per un mondo in cui si lavora ovunque

Per le organizzazioni è indispensabile trovare un modo per stare sempre un passo avanti rispetto al panorama delle minacce in evoluzione.

Insomma, quali sono le implicazioni del ricorso sempre più massiccio al lavoro da remoto? Sono due:

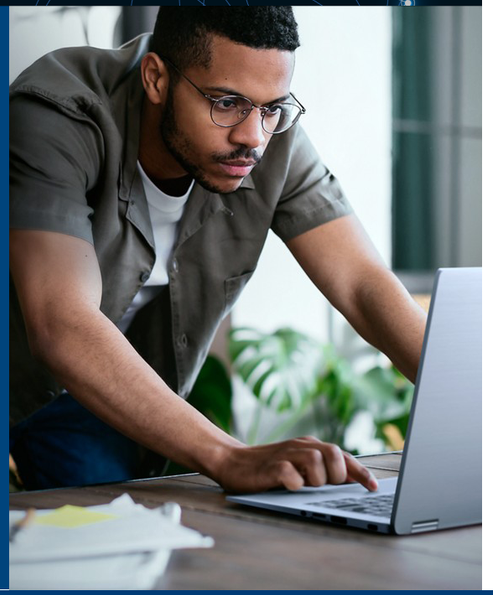
Tutte le organizzazioni sono vulnerabili...

> "[S]e qualcuno è ben deciso ad accedere al tuo sistema, ha probabilità di successo molto alte."
>
> — *Admiral Michael Rogers, ex direttore della National Security Agency ed ex comandante dello U.S. Cyber Command*[iii]

...e talvolta gli errori costano molto cari.

> "Raggiungendo il massimo storico, il costo di una violazione dei dati è stato in media di $ 4,88 milioni nel 2024."[iv]

I vettori di attacco sono in aumento, le superfici di attacco si espandono e per le aziende è impossibile essere completamente protette. È indispensabile che le organizzazioni ipotizzino lo scenario peggiore e rinforzino le difese per affrontare l'inevitabile attacco.



Il **69% delle organizzazioni** ha riscontrato una qualche tipologia di attacco informatico, a causa di asset con connessione a Internet gestiti in modo inadeguato.[v]

L'evoluzione delle strategie di sicurezza è cruciale

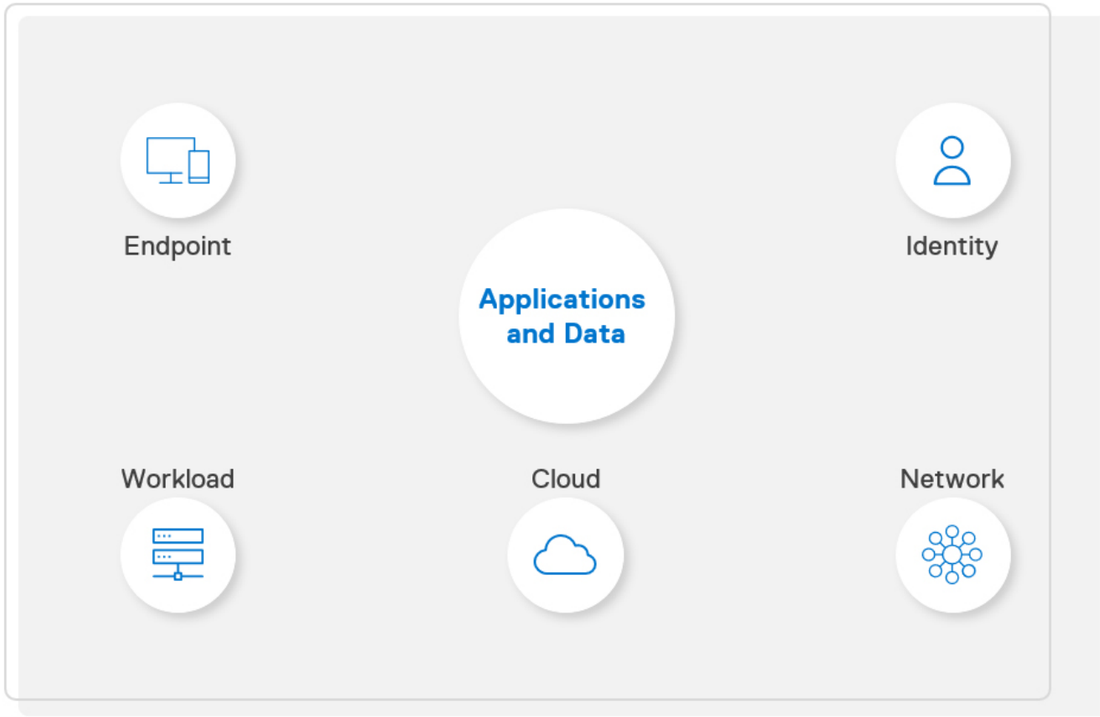
Bisogna adottare l'ambiente basato sul cloud. Ed è qui che entra in gioco Zero Trust.

I modelli di sicurezza tradizionali sono ormai inefficaci. Ecco perché.

Per salvaguardare l'efficacia del profilo di sicurezza della propria organizzazione, occorre tenere conto di cinque punti di controllo: endpoint, carico di lavoro, identità, rete e cloud. L'obiettivo è proteggere le applicazioni e i dati.

Gli approcci tradizionali sono spesso frammentati in silos, il che espone maggiormente agli attacchi le organizzazioni che se ne avvalgono.

Poi...

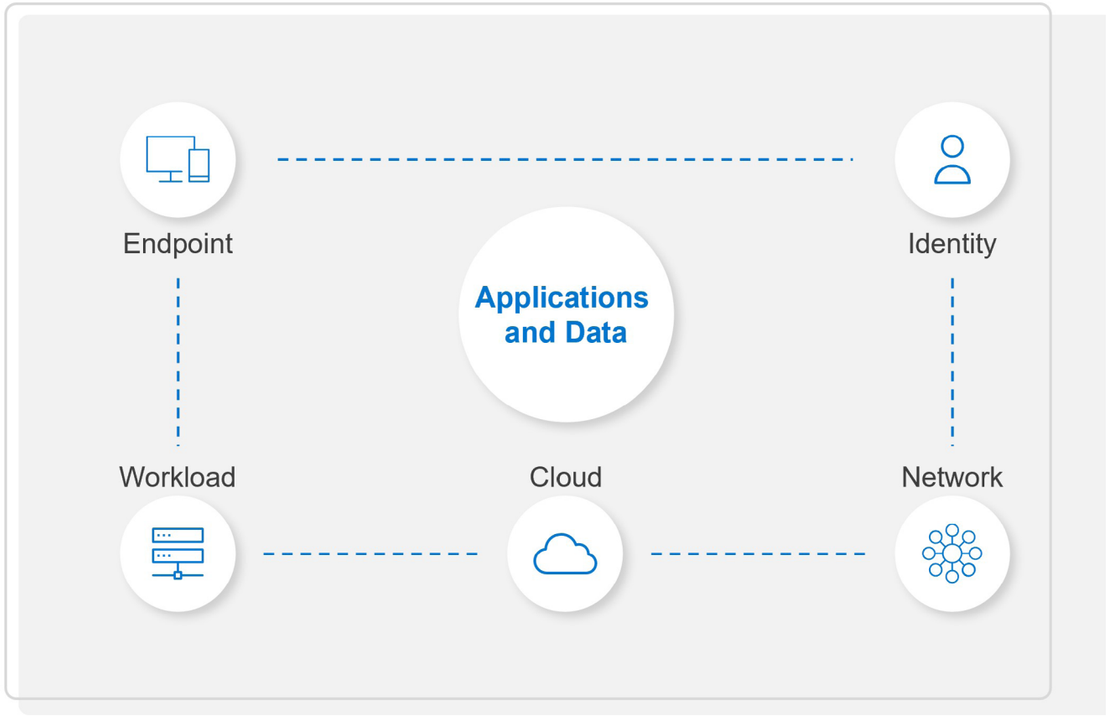


L'evoluzione delle strategie di sicurezza è cruciale

Bisogna adottare l'ambiente basato sul cloud. Ed è qui che entra in gioco Zero Trust.

Gli approcci moderni vantano un maggiore controllo e una migliore comunicazione tra i punti di controllo, ma con l'adozione di un ambiente di lavoro sempre più remoto/ibrido, bisogna rafforzare ulteriormente il perimetro.

Poi...

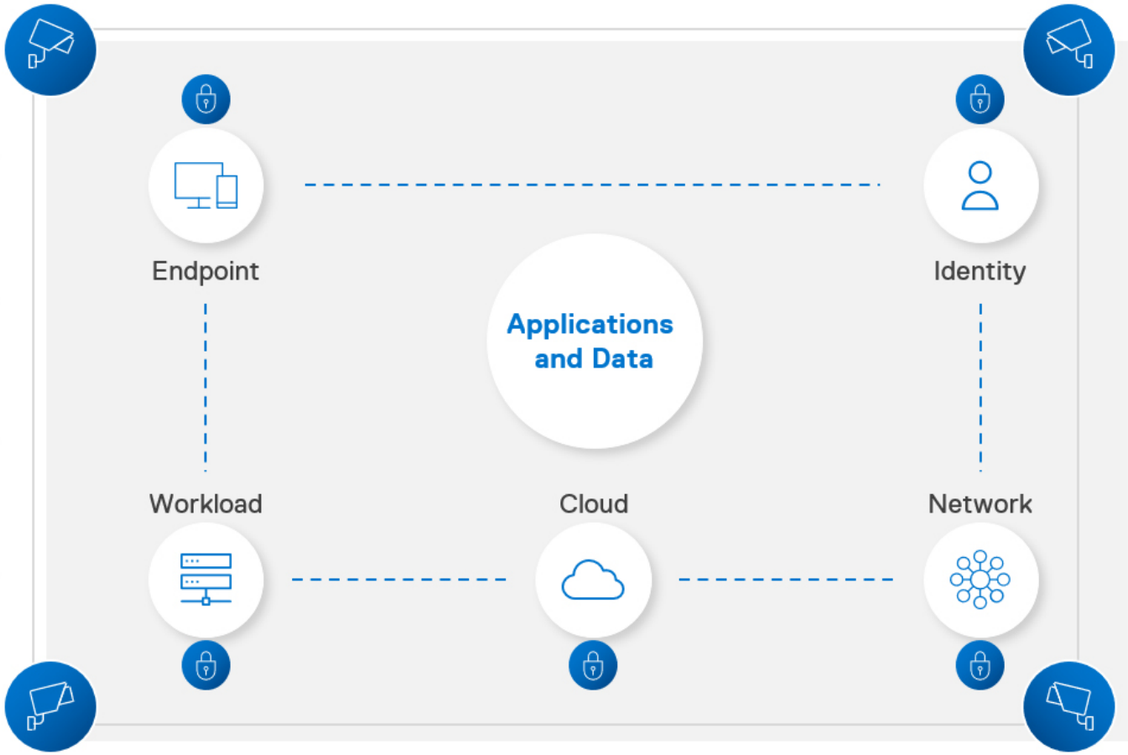


L'evoluzione delle strategie di sicurezza è cruciale

Bisogna adottare l'ambiente basato sul cloud. Ed è qui che entra in gioco Zero Trust.

Oggi i dipendenti lavorano ovunque, a casa, al bar, in hotel, e spesso utilizzano reti Wi-Fi non protette, prive o con limitata connettività ai data center e agli uffici protetti dai firewall. La soluzione predefinita sarebbe la connessione diretta a Internet dai loro dispositivi, in caso di collegamento ai file server sul cloud e alle applicazioni software as-a-Service (SaaS) e di lavoro con i dati aziendali.

Con l'aumento della sofisticazione degli attacchi e del numero dei vettori di attacco, le strategie di sicurezza tradizionali basate sulla fiducia implicita sono ormai inefficaci. Ed è qui che entra in gioco Zero Trust.



I concetti base di Zero Trust

Zero Trust è un nuovo modo di concepire la sicurezza. Sostituisce la fiducia *implicita* in base alla quale, una volta autenticati, gli utenti possono muoversi liberamente all'interno della rete. Zero Trust ribalta il paradigma per offrire alle organizzazioni il controllo esplicito dell'ambiente IT.

Per illustrare Zero Trust, partiamo dal ben noto concetto di creazione dei protocolli di sicurezza.

Tu lavori in ufficio presso un'azienda. Quando hai iniziato a farne parte, hai ricevuto un badge e hai imparato i protocolli di sicurezza. Ogni giorno entri nell'edificio. Ci sono telecamere ovunque. Passi il badge in diversi punti. Appena ti siedi alla scrivania, sblocchi il computer con una password.

An employee arrives at their office building and gets their badge out to gain entry.

Poi...

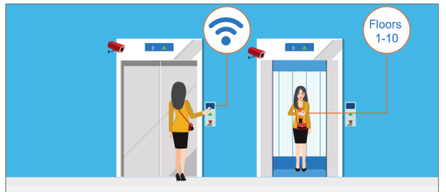
I concetti base di Zero Trust

Zero Trust è un nuovo modo di concepire la sicurezza. Sostituisce la fiducia *implicita* in base alla quale, una volta autenticati, gli utenti possono muoversi liberamente all'interno della rete. Zero Trust ribalta il paradigma per offrire alle organizzazioni il controllo esplicito dell'ambiente IT.

Per illustrare Zero Trust, partiamo dal ben noto concetto di creazione dei protocolli di sicurezza.

Tu lavori in ufficio presso un'azienda. Quando hai iniziato a farne parte, hai ricevuto un badge e hai imparato i protocolli di sicurezza. Ogni giorno entri nell'edificio. Ci sono telecamere ovunque. Passi il badge in diversi punti. Appena ti siedi alla scrivania, sblocchi il computer con una password.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

Poi...

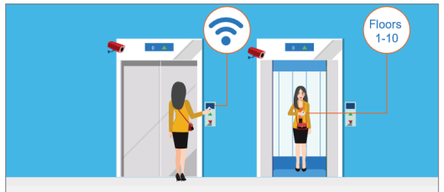
I concetti base di Zero Trust

Zero Trust è un nuovo modo di concepire la sicurezza. Sostituisce la fiducia *implicita* in base alla quale, una volta autenticati, gli utenti possono muoversi liberamente all'interno della rete. Zero Trust ribalta il paradigma per offrire alle organizzazioni il controllo esplicito dell'ambiente IT.

Per illustrare Zero Trust, partiamo dal ben noto concetto di creazione dei protocolli di sicurezza.

Tu lavori in ufficio presso un'azienda. Quando hai iniziato a farne parte, hai ricevuto un badge e hai imparato i protocolli di sicurezza. Ogni giorno entri nell'edificio. Ci sono telecamere ovunque. Passi il badge in diversi punti. Appena ti siedi alla scrivania, sblocchi il computer con una password.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.

Poi...

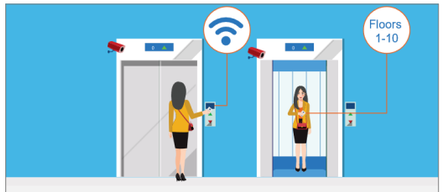
I concetti base di Zero Trust

Zero Trust è un nuovo modo di concepire la sicurezza. Sostituisce la fiducia *implicita* in base alla quale, una volta autenticati, gli utenti possono muoversi liberamente all'interno della rete. Zero Trust ribalta il paradigma per offrire alle organizzazioni il controllo esplicito dell'ambiente IT.

Per illustrare Zero Trust, partiamo dal ben noto concetto di creazione dei protocolli di sicurezza.

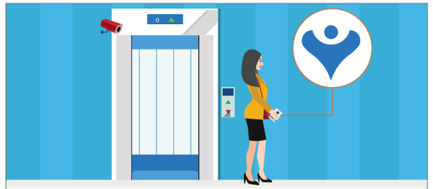
Tu lavori in ufficio presso un'azienda. Quando hai iniziato a farne parte, hai ricevuto un badge e hai imparato i protocolli di sicurezza. Ogni giorno entri nell'edificio. Ci sono telecamere ovunque. Passi il badge in diversi punti. Appena ti siedi alla scrivania, sblocchi il computer con una password.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

Poi...

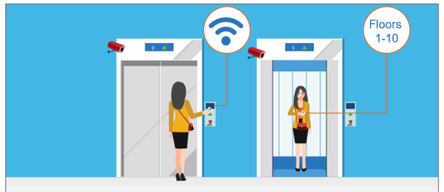
I concetti base di Zero Trust

Zero Trust è un nuovo modo di concepire la sicurezza. Sostituisce la fiducia *implicita* in base alla quale, una volta autenticati, gli utenti possono muoversi liberamente all'interno della rete. Zero Trust ribalta il paradigma per offrire alle organizzazioni il controllo esplicito dell'ambiente IT.

Per illustrare Zero Trust, partiamo dal ben noto concetto di creazione dei protocolli di sicurezza.

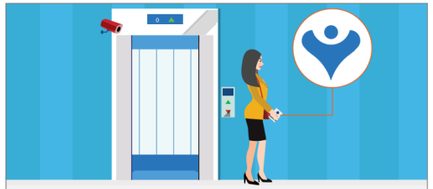
Tu lavori in ufficio presso un'azienda. Quando hai iniziato a farne parte, hai ricevuto un badge e hai imparato i protocolli di sicurezza. Ogni giorno entri nell'edificio. Ci sono telecamere ovunque. Passi il badge in diversi punti. Appena ti siedi alla scrivania, sblocchi il computer con una password.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

Poi...

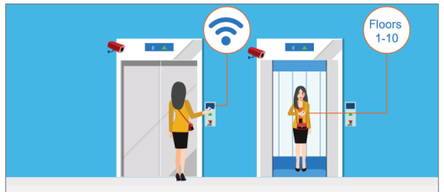
I concetti base di Zero Trust

Zero Trust è un nuovo modo di concepire la sicurezza. Sostituisce la fiducia *implicita* in base alla quale, una volta autenticati, gli utenti possono muoversi liberamente all'interno della rete. Zero Trust ribalta il paradigma per offrire alle organizzazioni il controllo esplicito dell'ambiente IT.

Per illustrare Zero Trust, partiamo dal ben noto concetto di creazione dei protocolli di sicurezza.

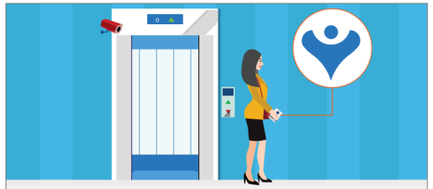
Tu lavori in ufficio presso un'azienda. Quando hai iniziato a farne parte, hai ricevuto un badge e hai imparato i protocolli di sicurezza. Ogni giorno entri nell'edificio. Ci sono telecamere ovunque. Passi il badge in diversi punti. Appena ti siedi alla scrivania, sblocchi il computer con una password.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

Poi...

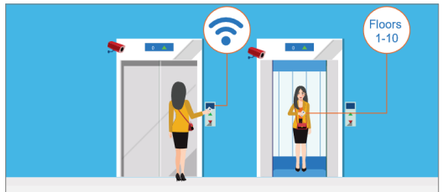
I concetti base di Zero Trust

È così che funziona Zero Trust.

Il tuo datore di lavoro ti ha identificato il primo giorno di impiego. Da allora ogni accesso che hai richiesto è stato verificato per proteggere gli asset dell'organizzazione (utenti, dati, ecc.). Per incrementare ulteriormente la sicurezza, ci sono guardie che osservano sui monitor tutto ciò che avviene all'interno dell'edificio ed esaminano qualsiasi comportamento insolito, ad esempio tentativi di accesso in stanze per le quali non si dispone dell'autorizzazione.

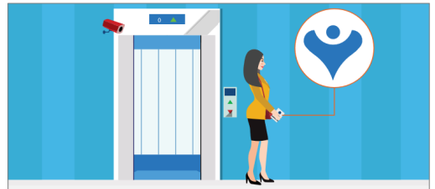
Al giorno d'oggi, utenti, dispositivi, applicazioni e dati si trovano con sempre maggiore frequenza al di fuori delle reti aziendali. Ecco perché l'identità degli utenti è diventata un punto cieco e la sua compromissione costituisce l'elemento chiave della maggior parte delle violazioni. Zero Trust risolve il problema.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

Attivazione dei principi Zero Trust

La sicurezza degli endpoint è un elemento essenziale della trasformazione Zero Trust.

Per adottare con successo una strategia Zero Trust, è indispensabile proteggere gli endpoint.

In base al framework MITRE ATT&CK®, oggi sono ben nove le "tecniche di accesso iniziali" di cui gli avversari si avvalgono per avere accesso alle reti *(vedere l'illustrazione)*.[vi] Come dimostra la ricerca, in questo mondo basato sul cloud, le difese tradizionali sono insufficienti per la protezione degli endpoint. Al malintenzionato basta un solo punto di accesso. Con gli endpoint, ci sono decine di vulnerabilità da sfruttare nell'intero ciclo di vita del dispositivo.

Con l'incremento del numero di dispositivi presenti su una rete, gli endpoint diventano vettori di attacco sempre più esposti.

Le policy di sicurezza del modello Zero Trust definiscono in modo molto dettagliato gli accessi "riconosciuti sicuri" e bloccano tutto il resto. Quindi la gestione delle minacce monitora eventuali deviazioni rispetto agli accessi "riconosciuti sicuri", segnala i comportamenti anomali e avvia le misure adeguate per correggere la potenziale minaccia.

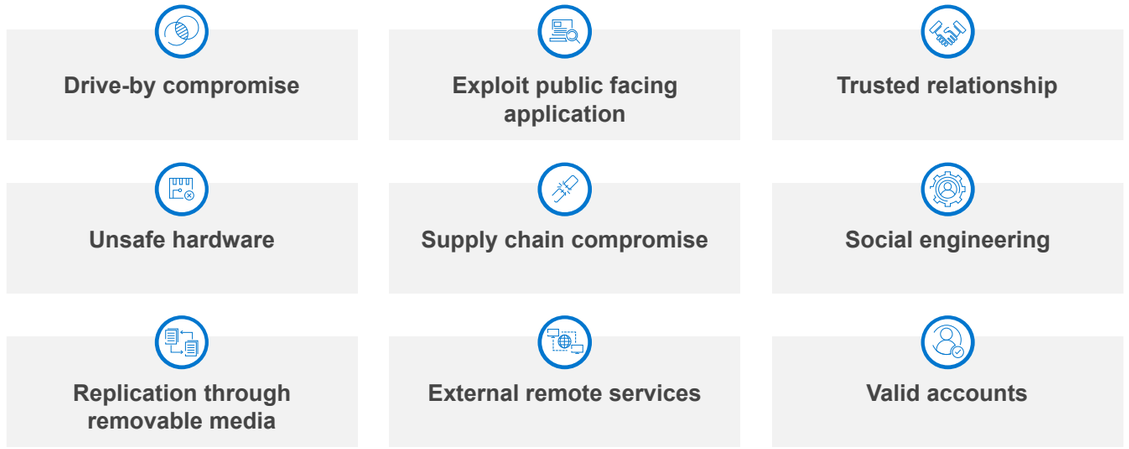


Illustrazione 1/3

Attivazione dei principi Zero Trust

La sicurezza degli endpoint è un elemento essenziale della trasformazione Zero Trust.

Per adottare con successo una strategia Zero Trust, è indispensabile proteggere gli endpoint.

In base al framework MITRE ATT&CK®, oggi sono ben nove le "tecniche di accesso iniziali" di cui gli avversari si avvalgono per avere accesso alle reti *(vedere l'illustrazione)*.[vi] Come dimostra la ricerca, in questo mondo basato sul cloud, le difese tradizionali sono insufficienti per la protezione degli endpoint. Al malintenzionato basta un solo punto di accesso. Con gli endpoint, ci sono decine di vulnerabilità da sfruttare nell'intero ciclo di vita del dispositivo.

Con l'incremento del numero di dispositivi presenti su una rete, gli endpoint diventano vettori di attacco sempre più esposti.

Le policy di sicurezza del modello Zero Trust definiscono in modo molto dettagliato gli accessi "riconosciuti sicuri" e bloccano tutto il resto. Quindi la gestione delle minacce monitora eventuali deviazioni rispetto agli accessi "riconosciuti sicuri", segnala i comportamenti anomali e avvia le misure adeguate per correggere la potenziale minaccia.

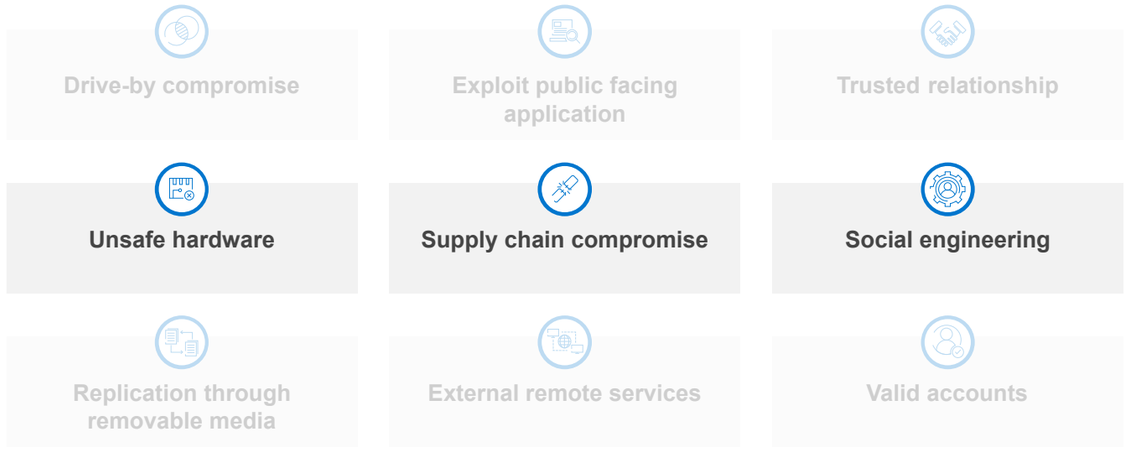


Illustrazione 2/3

Attivazione dei principi Zero Trust

La sicurezza degli endpoint è un elemento essenziale della trasformazione Zero Trust.

Per adottare con successo una strategia Zero Trust, è indispensabile proteggere gli endpoint.

In base al framework MITRE ATT&CK®, oggi sono ben nove le "tecniche di accesso iniziali" di cui gli avversari si avvalgono per avere accesso alle reti *(vedere l'illustrazione)*.[vi] Come dimostra la ricerca, in questo mondo basato sul cloud, le difese tradizionali sono insufficienti per la protezione degli endpoint. Al malintenzionato basta un solo punto di accesso. Con gli endpoint, ci sono decine di vulnerabilità da sfruttare nell'intero ciclo di vita del dispositivo.

Con l'incremento del numero di dispositivi presenti su una rete, gli endpoint diventano vettori di attacco sempre più esposti.

Le policy di sicurezza del modello Zero Trust definiscono in modo molto dettagliato gli accessi "riconosciuti sicuri" e bloccano tutto il resto. Quindi la gestione delle minacce monitora eventuali deviazioni rispetto agli accessi "riconosciuti sicuri", segnala i comportamenti anomali e avvia le misure adeguate per correggere la potenziale minaccia.

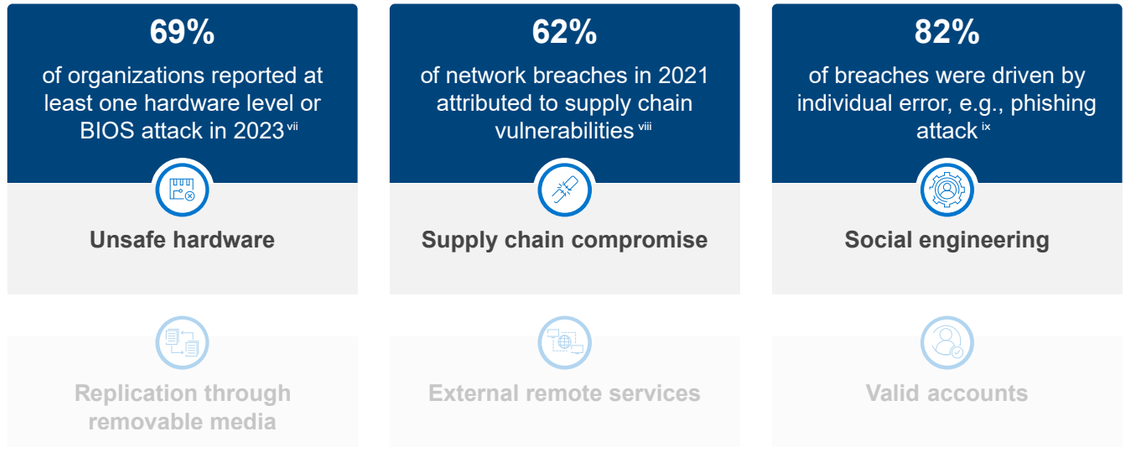


Illustrazione 3/3

Tre consigli per preparare la strategia Zero Trust

Prepara la tua organizzazione alla riuscita della trasformazione Zero Trust.

1

Stabilisci le policy e i controlli giusti per le tue priorità di business.

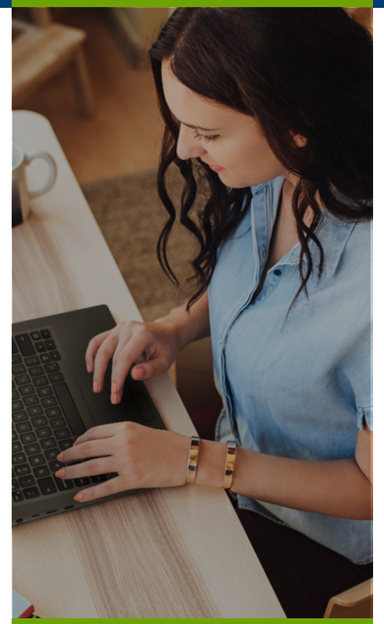
I policy engine e la gestione delle policy sono fondamentali per l'efficacia delle implementazioni Zero Trust, tuttavia le organizzazioni dispongono di budget limitati per la sicurezza, quindi il primo passo è determinare le priorità di business. Quali sono i principali asset e IP da proteggere? Soppesa la superficie di attacco rispetto al rischio ammissibile per l'organizzazione.

A questo punto, rivedi le policy e i controlli attualmente in vigore. Oggi i rischi hanno origine dal mondo basato sul cloud in cui viviamo. Il tuo policy engine ne tiene conto?

Con l'introduzione di policy finalizzate a disciplinare l'accesso agli asset di maggiore importanza, è possibile espandere la portata del tuo intervento.

SCOPRI DI PIÙ

Per maggiori informazioni, *guarda questo video* nel quale gli esperti informatici Dell parlano dei principali rischi per la sicurezza che le organizzazioni si trovano ad affrontare oggi.



Con un numero sempre maggiore di utenti, applicazioni, dati e dispositivi al di fuori della rete aziendale, l'**82%** dei responsabili delle decisioni in materia di sicurezza IT sostiene di essere stato costretto a rivalutare le policy di sicurezza.[x]

Tre consigli per preparare la strategia Zero Trust

Prepara la tua organizzazione alla riuscita della trasformazione Zero Trust.

2 Parti dalla protezione dei dispositivi.

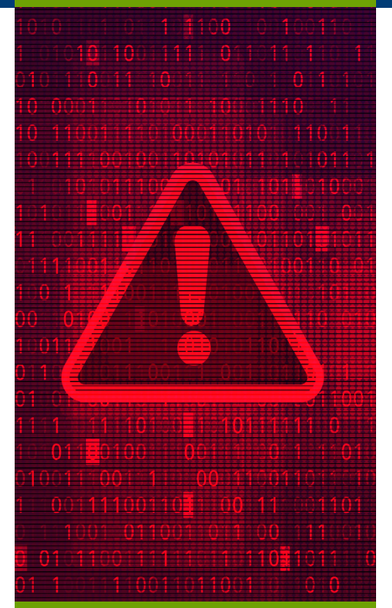
Pianifica il percorso Zero Trust su solide basi. Rafforza le difese utilizzando dispositivi progettati e sviluppati per la sicurezza, tra cui:

A. **Protezioni basate su hardware e firmware** che tutelano lo stack degli endpoint e consentono la visibilità (ad esempio rilevano l'eventuale compromissione del BIOS e avvisano il team IT). Dota la tua organizzazione delle tecnologie di verifica dell'identità per ogni nuova richiesta di accesso, con il minimo impatto possibile sulla produttività dei dipendenti.

B. **Protezioni della supply chain e controlli dell'integrità** che tutelano ogni fase del ciclo di vita dei PC. Come abbiamo rilevato negli ultimi anni, talvolta gli attacchi ai danni della supply chain sono devastanti. Per creare una vera architettura Zero Trust, l'autenticazione, la verifica e il monitoraggio partono dalla supply chain. Collabora con vendor che 1) adottano prassi sicure e 2) offrono l'opportunità di convalidare l'integrità dei dispositivi, dal procurement alla produzione fino alla consegna.

SCOPRI DI PIÙ

Per maggiori informazioni sulle best practice di sicurezza dei dispositivi, leggi il white paper Dell e Intel, Achieving Pervasive Security Above and Below the OS.



Nel **2021**, un'azienda di gestione IT ha diffuso un attacco ransomware ad almeno **1.500** clienti.[xi]

Tre consigli per preparare la strategia Zero Trust

Prepara la tua organizzazione alla riuscita della trasformazione Zero Trust.

3

Impegnati per la perfetta integrazione e interoperabilità nel tuo ecosistema.

Per ottenere un profilo di sicurezza efficace ad alti livelli, vi sono tre aspetti essenziali:

A. integrazione di tutte le difese nell'ecosistema IT;

B. visibilità in tempo reale;

C. possibilità di intervenire se necessario.

In questo mondo basato sul cloud, dove anche la minima vulnerabilità trascurata è potenzialmente pericolosa, è importante che tutti i sistemi riconoscano le potenziali minacce *e* siano pronti ad adottare le misure necessarie.

I tuoi sistemi sono integrati o funzionano in silos? Il tuo policy engine attiva un flusso di lavoro specifico quando l'amministratore IT riceve un avviso di corruzione del BIOS sulla rete? In un ambiente integrato, sarebbe necessario che le automazioni mettessero immediatamente in quarantena il BIOS in questione, limitassero ulteriori accessi ed eseguissero una prova di applicazione delle patch.

Hai visibilità su tutti gli endpoint? L'ideale sarebbe disporre di ricchi sistemi di telemetria attivi su ogni livello, dalla supply chain (ad esempio la zona di carico) al firmware (ad esempio gli avvisi di manomissione del BIOS).

Ma l'efficacia della telemetria va di pari passo con quella delle integrazioni. Hai la possibilità di utilizzare i dati? È importante disporre delle risorse giuste, ad esempio personale competente per la sicurezza informatica, al fine di interpretare i dati e i flussi di lavoro dei programmi per la risoluzione dei problemi.

Il 41% delle organizzazioni è impegnato nell'implementazione di Zero Trust[xii]

DELL Technologies

Messaggi principali

Il futuro della sicurezza è Zero Trust.

- Con l'adozione dell'ambiente di lavoro del futuro, i vettori di attacco si sono moltiplicati.
- Le violazioni sono inevitabili. Riduci al minimo la superficie di attacco con difese che preparano allo scenario peggiore.
- Zero Trust è un nuovo modo di concepire la sicurezza, che offre alle organizzazioni un controllo esplicito dell'ambiente IT.
- Le protezioni degli endpoint che attivano i principi Zero Trust sono cruciali per mantenere fondamenta moderne e protette.
- Individua gli asset principali cui dare la priorità nella creazione dell'architettura Zero Trust.
- Acquisisci i dispositivi da vendor che offrono protezioni integrate ed effettuano investimenti importanti sui controlli della supply chain.
- Valuta la sicurezza e l'interoperabilità IT. Continua a integrare i flussi di lavoro per rafforzare il tuo profilo di sicurezza.

Passa alla fase successiva

Quello della sicurezza è un argomento che incute timore alle organizzazioni di tutte le dimensioni. Scegli un partner esperto in materia di sicurezza e tecnologia per semplificare la trasformazione Zero Trust.

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 basato sulla difesa contrasta le minacce con la combinazione di protezioni integrate e vigilanza costante. Gli utenti finali rimangono produttivi e il team IT tiene alta la fiducia con le soluzioni di sicurezza pensate per il mondo di oggi basato sul cloud.

Contattaci: global.security.sales@dell.com
Visita il sito: Dell.com/Endpoint-Security
Seguici su: LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac 2nd Edition. Cybersecurity Ventures, 2022 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute e IBM, Cost of a Data Breach Report, 2024 https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked. Plan Now: Cybersecurity in Health Care, 2021 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute e IBM, Cost of a Data Breach Report, 2024 https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results, Security Hygiene and Posture Management, 2022 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum Group, Endpoint Security Trends, 2023. https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/futurum-group-endpoint-security-trends-research-report.pdf

[viii] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute Endpoint Risk Report, 2021 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget, 2021 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute e IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach