DELL Technologies

Zero Trust
Il percorso per migliorare la sicurezza informatica

Intraprendi il percorso Zero Trust affiancandoti a un partner esperto di tecnologia e sicurezza.

Per sviluppare la propria maturità in termini di sicurezza informatica, le organizzazioni mettono a punto una roadmap pratica che indichi in che modo è possibile ridurre la superficie di attacco, rilevare e rispondere alle minacce informatiche, nonché implementare soluzioni per eseguire il ripristino dagli attacchi informatici, il tutto con le funzionalità Zero Trust.

Per affrontare le minacce informatiche, che diventano sempre più sofisticate, Dell si avvale delle funzionalità di sicurezza integrate nelle nostre soluzioni e del supporto dei partner, affinché i clienti realizzino l'approccio Zero Trust, nel rispetto dei loro obiettivi aziendali.

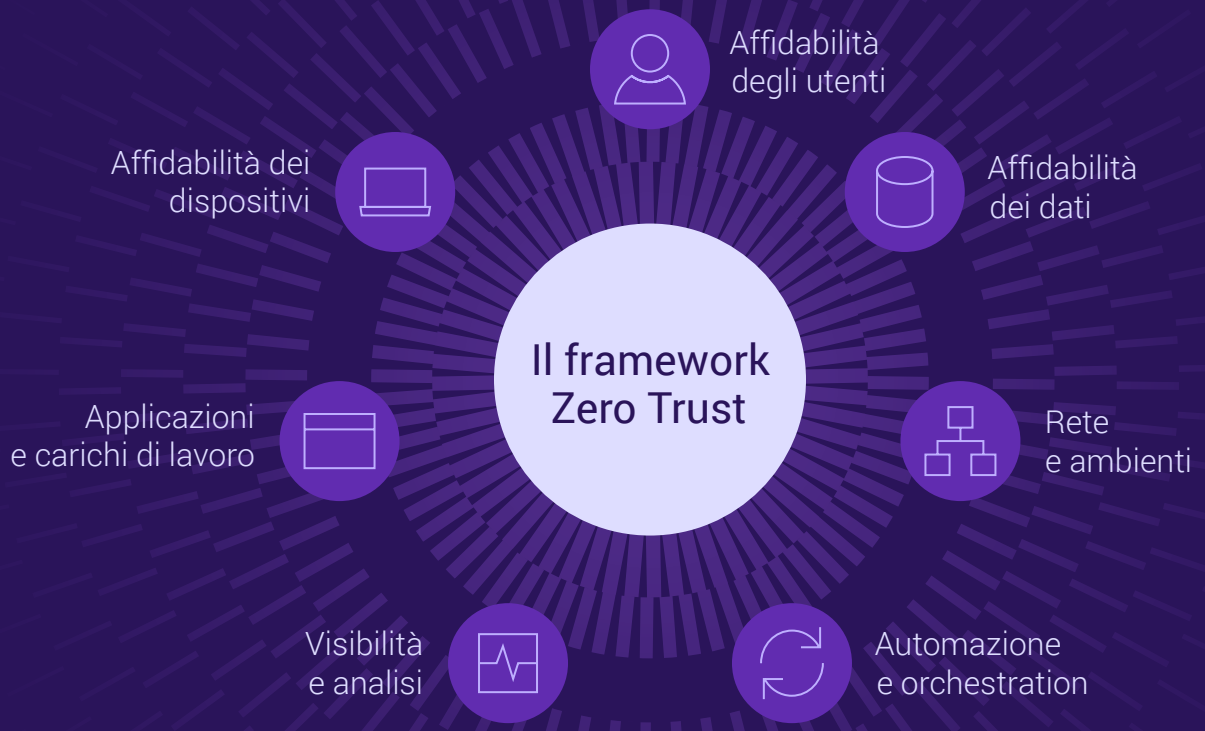
Che cos'è Zero Trust?

Immagina la tua rete come se fosse un castello. Se il ponte levatoio è abbassato e qualcuno prova a entrare poi potrà muoversi liberamente. È giunto il momento di aggiornare il modello di sicurezza basato sulla difesa perimetrale al framework Zero Trust, più moderno e più sicuro.

Zero Trust è un approccio architetturale alla sicurezza, più che un prodotto da acquistare. Il framework diffida di qualsiasi attività e verifica sistematicamente la legittimità degli impieghi aziendali prima di concedere l'accesso alle risorse a qualcuno o qualcosa. Quindi gli utenti e i dispositivi non sono ritenuti affidabili a priori, anche se connessi a reti autorizzate e verificati in precedenza.

Mai fidarsi; verificare in ogni caso.

Nozioni fondamentali per la sicurezza dell'ecosistema IT.



Il framework Zero Trust, come definito dal National Institute of Standards and Technologies (NIST), è stato adottato e integrato in un'architettura del Dipartimento della Difesa degli Stati Uniti.

Il framework include sette pilastri correlati che orientano Dell Technologies in tutti gli ambiti legati alla sicurezza. Combinando i pilastri, l'architettura assume una struttura multiforme e integrata, da cui deriva l'approccio alla sicurezza completo che protegge i dati e l'infrastruttura delle organizzazioni.

L'adozione di Zero Trust si è rivelata impegnativa, data la complessità posta dall'integrazione delle diverse funzionalità di sicurezza e dalla navigazione tra le opzioni frammentate di vari provider di sicurezza.

NIST

U.S. Department *of* Defense

DELL Technologies

Sviluppo della maturità Zero Trust.

Indipendentemente dal punto in cui ti trovi nel percorso, Dell ti propone soluzioni utili.

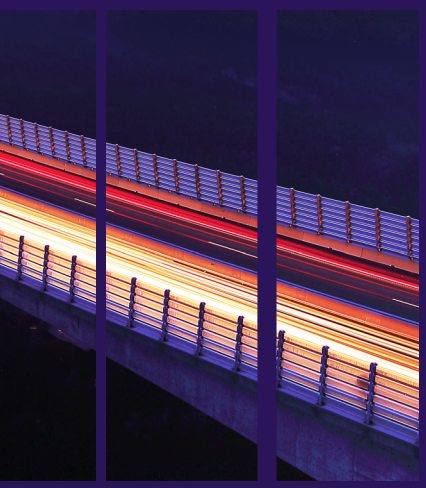
Dell Technologies offre possibilità di scelta e flessibilità alla tua organizzazione. Se miri a far progredire la maturità della sicurezza informatica, sfrutta le nostre soluzioni di sicurezza con funzionalità Zero Trust, utili per migliorare le capacità di resistenza, rilevamento, difesa e ripristino da attività informatiche malevole.

Attivazione dei principi Zero Trust.

Abilita le possibilità di scelta e la flessibilità per l'avanzamento della maturità della sicurezza informatica.

Dell Technologies offre soluzioni di sicurezza e funzionalità Zero Trust che migliorano le capacità di resistenza, rilevamento, difesa e ripristino da attività informatiche malevole. In questo modo disponi di:

- protezioni integrate che migliorano l'automazione, la Threat Intelligence, l'autenticazione, la visibilità e altro ancora
- servizi per lo sviluppo di roadmap, integrazione di tecnologie chiave e gestione proattiva a supporto di Zero Trust
- servizi di consulenza professionali, gestiti e sulla sicurezza
- ampio ecosistema dei partner



Adozione estremamente semplificata di Zero Trust.

Scegli senza riserve l'architettura completamente integrata.

Il modello Zero Trust, in qualità di approccio architetturale alla sicurezza, non prevede un singolo prodotto, bensì richiede l'attenta pianificazione di soluzioni in sintonia tra di loro. Dell rimuove l'onere dell'integrazione Zero Trust operando come segue:

- Dell costruisce la prima e unica architettura Zero Trust completamente integrata, progettata, testata e convalidata dal Dipartimento della Difesa degli Stati Uniti

DELL Technologies

Attivazione dei principi Zero Trust.

Realizza l'approccio Zero Trust partendo dal tuo ecosistema di sicurezza specifico.

Dell contribuisce all'avanzamento della maturità della sicurezza informatica a supporto delle strategie Zero Trust, funzionali per ridurre la superficie di attacco, migliorare il rilevamento e velocizzare il ripristino dalle minacce informatiche.

Ciascun pilastro Zero Trust racchiude tecnologie, processi e persone in base alle aree critiche in cui occorrono policy aziendali e di sicurezza per proteggere l'organizzazione. I Dell Security Services sono utili per:

- La maturità della sicurezza, Zero Trust e gli assessment dei rischi
- L'elaborazione di strategie e roadmap
- I servizi gestiti delle funzionalità chiave di Zero Trust

DELL Technologies

Fondamenta di Zero Trust.

Forniamo soluzioni di sicurezza avanzate e integrate che ti offrono un vantaggio sul percorso Zero Trust.

Dell Data Protection

Vault di Cyber Recovery | PowerProtect Data Manager | CyberSense Transparent Snapshot | CloudIQ | Blocco del sistema | Rilevamento delle deviazioni | Gestione delle chiavi sicura a livello aziendale | TLS 1.3 | IPv6 | Autenticazione a più fattori | Single Sign-on | Accesso basato sui ruoli | CloudIQ

Server Dell PowerEdge

Distinta base del software | Verifica dei componenti protetti | Silicon Root of Trust | Blocco del sistema | Rilevamento delle deviazioni | Gestione delle chiavi sicura a livello aziendale | TLS 1.3 | IPv6 | Autenticazione a più fattori | Single sign-on | Accesso basato sui ruoli | CloudIQ

Piattaforme di storage Dell

Isolamento dei dati | Immutabilità dei dati | Rilevamento delle minacce | Autenticazione per il controllo degli accessi | Crittografia dei dati | Rafforzamento STIG | Root of Trust hardware | Avvio sicuro | Firmware con firma digitale | Accesso basato sui ruoli | Snapshot protette

Dell HCI/CI

Root of Trust hardware | Catena di attendibilità dell'avvio sicuro | Aggiornamenti con firma digitale | Gestione delle chiavi | Registrazione protetta | Switch virtuali distribuiti | Isolamento VM | Autenticazione e autorizzazione | Connettori dell'ecosistema | Convalida continua degli stati | Integrità del codice software | Matrice di compatibilità elettronica

PC commerciali Dell

Sicurezza BIOS/firmware | Sicurezza hardware | Garanzia della supply chain | Software per la gestione delle minacce (EDR, XDR, VDR) | Software per la protezione dei dati in rete e nel cloud

Soluzioni edge Dell

Attestazione hardware/software/VM | Onboarding protetto | Catena di affidabilità | Distribuzione protetta di OS/applicazioni | Gestione dei diritti ai dati

Dell Network Switch

SmartFabric | CloudIQ | SD-WAN | Segmentazione VLAN | Enterprise SONiC | ACL | RADIUS | TACACS+ | Crittografia | Rafforzamento switch | Micro-segmentazione | Routing e inoltro virtuali

DELL Technologies

Il nostro approccio accelerato.

Veloce e accurato, il progetto Fort Zero integra Zero Trust in tutta l'organizzazione in modo olistico.

Il progetto Fort Zero offre un metodo convalidato per l'avanzamento immediato della maturità Zero Trust, riducendo i tempi di adozione, limitando le interruzioni e gestendo i costi.

Alla luce delle nostre competenze e della nostra portata nell'industria, il Dipartimento della Difesa degli Stati Uniti ha chiesto a Dell Technologies di contribuire ad accelerare l'adozione dell'approccio Zero Trust. Per supportare le organizzazioni del settore pubblico e privato a semplificare l'adozione dell'architettura Zero Trust e a dimensionarla a livello globale, Dell lavora alla realizzazione di un ecosistema apposito e guida l'integrazione del framework in oltre 30 aziende leader del settore della tecnologia e della sicurezza. Siamo leader nello sviluppo e nel dimensionamento globale dell'architettura Zero Trust, sia per le organizzazioni private che per quelle pubbliche in tutto il mondo. Questo dimostra l'impegno di Dell nel quadro degli obiettivi per realizzare l'approccio Zero Trust, perseguiti dal Dipartimento della Difesa degli Stati Uniti.

On-premise

Nei data center, per le organizzazioni in cui la sicurezza e la conformità dei dati sono fondamentali.

Da remoto o a livello regionale

In sedi come punti di vendita al dettaglio in cui le analisi sicure e in tempo reale dei dati dei clienti sono utili per offrire un vantaggio competitivo.

Edge rimovibile

In luoghi come aerei o veicoli dotati di connettività intermittente, dove è necessaria l'implementazione temporanea per garantire continuità operativa.

DELL Technologies

Ti aiutiamo ad accelerare l'adozione di Zero Trust implementando tutte le **152** attività portate avanti dal Dipartimento della Difesa degli Stati Uniti per conseguire un livello avanzato di protezione Zero Trust.

Enabler di esecuzione

Principi | Organizzazione | Formazione | Materiale | Leadership e istruzione | Personale | Strutture | Policy

Livello prefissato Zero Trust

Affidabilità degli utenti

- Inventario utenti
- Autorizzazione basata sulle applicazioni
- Accesso dinamico basato sulle regole (parte 1)
- MFA/IDP dell'organizzazione
- Implementazione del sistema e riduzione dei privilegi utenti (parte 1)
- Gestione del ciclo di vita dell'identità dell'organizzazione
- Utente negato per policy predefinita
- Autenticazione singola
- Implementazione del sistema e riduzione dei privilegi utenti (parte 2)
- Gestione del ciclo di vita dell'identità aziendale (parte 1)
- Implementazione degli strumenti UEBA
- Autenticazione periodica
- PKI/IDP aziendale (parte 1)

Affidabilità dei dispositivi

- Gap analysis dello strumento guida del dispositivo
- Integrazione degli antivirus di nuova generazione con C2C
- Dispositivo NPE/PKI in gestione
- Dispositivo negato per policy predefinita
- Implementazione di UEDM o strumenti equivalenti
- Gestione dei dispositivi aziendali (parte 1)
- Implementazione degli strumenti EDR e integrazione con C2C
- Implementazione degli strumenti di gestione di asset, vulnerabilità e patch
- IDP aziendale (parte 1)
- Implementazione dell'autorizzazione di rete basata sulla conformità/C2C (parte 1)
- Implementazione del controllo delle applicazioni e di strumenti FIM
- Supporto IoT e BYOD gestito e limitato
- Gestione dei dispositivi aziendali (parte 2)
- Implementazione degli strumenti XDR e integrazione con C2C (parte 1)

Applicazioni e carichi di lavoro

- Identificazione applicazione/codice
- Autorizzazione delle risorse (parte 1)
- Creazione del processo di sviluppo del software DevSecOps (parte 1)
- Binari/codice approvati
- Programma di gestione delle vulnerabilità (parte 1)
- Autorizzazione delle risorse SDC (parte 1)
- Autorizzazione delle risorse (parte 2)
- Creazione del processo di sviluppo del software DevSecOps (parte 2)
- Automatizzazione della sicurezza delle applicazioni e della correzione del codice (parte 1)
- Programma di gestione delle vulnerabilità (parte 2)
- Convalida continua
- Autorizzazione delle risorse SDC (parte 2)

Affidabilità dei dati

- Analisi dei dati
- Registrazione e analisi dei punti di applicazione DLP
- Registrazione e analisi dei punti di applicazione DRM
- Definizione degli standard di etichettatura dei dati
- Implementazione degli strumenti di etichettatura e classificazione dei dati
- Monitoraggio delle attività dei file (parte 1)
- Implementazione degli strumenti DRM e di protezione (parte 1)
- Implementazione dei punti di applicazione
- Standard di interoperabilità
- Sviluppo di policy di SDS
- Etichettatura dei dati manuale (parte 1)
- Monitoraggio delle attività dei file (parte 2)
- Implementazione degli strumenti DRM e di protezione (parte 2)
- Implementazione DLP tramite etichette e analisi dei dati (parte 1)
- Integrazione dell'accesso DAAS con policy SDS (parte 1)
- Implementazione DRM tramite etichette e analisi dei dati (parte 1)
- Integrazione di una o più soluzioni di SDS e policy con IDP aziendale (parte 1)

Rete e ambienti

- Definizione delle regole e delle policy di accesso per il controllo granulare (parte 1)
- Definizione degli API SDN
- Definizione delle regole e delle policy di accesso per il controllo granulare (parte 2)
- Implementazione dell'infrastruttura programmabile SDN
- Macro-segmentazione del data center
- Implementazione della micro-segmentazione
- Segmentazione dei flussi nei piani dati e di gestione del controllo
- Macro-segmentazione B/C/P/S
- Micro-segmentazione di applicazioni e dispositivi
- Protezione dei dati in transito

Automazione e orchestration

- Inventario e sviluppo delle policy
- Analisi dell'automazione delle attività
- Analisi dell'automazione delle risposte
- Analisi della conformità degli strumenti
- Profilo di accesso dell'organizzazione
- Implementazione degli strumenti SOAR
- Chiamate e schemi API standardizzati (parte 1)
- Miglioramento del workflow (parte 1)
- Profilo di sicurezza aziendale (parte 1)
- Integrazione aziendale e provisioning del workflow (parte 1)
- Implementazione degli strumenti ML di etichettatura e classificazione dei dati
- Chiamate e schemi API standardizzati (parte 2)
- Miglioramento del workflow (parte 2)

Visibilità e analisi

- Osservazioni sul dimensionamento
- Esame dei registri
- ID degli asset e correlazione degli avvisi
- Avvisi sulle minacce (parte 1)
- Implementazione degli strumenti di analisi
- Programma di Threat Intelligence informatica (parte 1)
- Analisi dei registri
- Avvisi sulle minacce (parte 2)
- Baseline utente/dispositivo
- Definizione del comportamento baseline degli utenti
- Baseline e profilazione (parte 1)
- Programma di Threat Intelligence informatica (parte 2)

Numero complessivo delle attività previste: 91

Fonte: Pubblicazione "DoD Zero Trust Strategy", 7 novembre 2022

DELL Technologies

Zero Trust avanzato

Affidabilità degli utenti

- Accesso dinamico basato sulle regole (parte 2)
- Ruoli e autorizzazioni aziendali (parte 1)
- MFA flessibile alternativa (parte 1)
- Approvazioni in tempo reale e analisi JIT/JEA (parte 1)
- Gestione del ciclo di vita dell'identità aziendale (parte 2)
- Monitoraggio delle attività degli utenti (parte 1)
- Autenticazione continua (parte 1)
- Autenticazione continua (parte 2)
- PKI/IDP aziendale (parte 3)
- Ruoli e autorizzazioni aziendali (parte 2)
- MFA flessibile alternativa (parte 2)
- Approvazioni in tempo reale e analisi JIT/JEA (parte 2)
- Gestione del ciclo di vita dell'identità aziendale (parte 3)
- Monitoraggio delle attività degli utenti (parte 2)
- PKI/IDP aziendale (parte 2)

Affidabilità dei dispositivi

- IDP aziendale (parte 2)
- Implementazione dell'autorizzazione di rete basata sulla conformità/C2C (parte 2)
- Monitoraggio delle attività delle entità (parte 1)
- Integrazione completa della sicurezza dei dispositivi in Slack con C2C
- PKI aziendale (parte 1)
- Supporto IoT e BYOD gestito e completo (parte 1)
- Implementazione degli strumenti XDR e integrazione con C2C (parte 2)
- Monitoraggio delle attività delle entità (parte 2)
- PKI aziendale (parte 2)
- Supporto IoT e BYOD gestito e completo (parte 2)

Applicazioni e carichi di lavoro

- Arricchimento degli attributi per l'autorizzazione delle risorse (parte 1)
- Arricchimento degli attributi per l'autorizzazione delle risorse (parte 2)
- Autorizzazione continua all'operatività (parte 1)
- Automatizzazione della sicurezza delle applicazioni e della correzione del codice (parte 2)
- Micro-segmenti API REST
- Autorizzazione continua all'operatività (parte 2)

Affidabilità dei dati

- Etichettatura dei dati manuale (parte 2)
- Monitoraggio dell'attività dei database
- Etichettatura dei dati e supporto automatizzati (parte 1)
- Implementazione DRM tramite etichette e analisi dei dati (parte 2)
- Implementazione DLP tramite etichette e analisi dei dati (parte 2)
- Integrazione dell'accesso DAAS con policy SDS (parte 2)
- Integrazione di una o più soluzioni di SDS e policy con IDP aziendale (parte 2)
- Integrazione dello strumento SOS e/o integrazione con strumento DRM (parte 1)
- Etichettatura dei dati e supporto automatizzati (parte 2)
- Monitoraggio completo delle attività dei dati
- Implementazione DRM tramite etichette e analisi dei dati (parte 3)
- Implementazione DLP tramite etichette e analisi dei dati (parte 3)
- Integrazione dell'accesso DAAS con policy SDS (parte 3)
- Integrazione dello strumento SDS e/o integrazione con strumento DRM (parte 2)

Rete e ambienti

- Rilevamento e ottimizzazione degli asset di rete
- Decisioni sugli accessi in tempo reale
- Micro-segmentazione dei processi

Automazione e orchestration

- Profilo di sicurezza aziendale (parte 2)
- Integrazione aziendale e provisioning del workflow (parte 2)
- Implementazione dello strumento di automazione dell'AI
- Miglioramento del workflow (parte 3)
- AI guidata dall'analisi per le decisioni sulle modifiche A&O
- Implementazione dei playbook
- Flussi di lavoro automatizzati

Visibilità e analisi

- Avvisi sulle minacce (parte 3)
- Baseline e profilazione (parte 2)
- Supporto baseline UEBA (parte 1)
- Supporto baseline UEBA (parte 2)
- Accesso alla rete abilitato per l'AI
- Controllo dinamico degli accessi abilitato per l'AI

Numero complessivo delle attività avanzate: **61**

Dell Technologies semplifica la complessità del percorso rapido verso la maturità Zero Trust.

Fonte: Pubblicazione "DoD Zero Trust Strategy", 7 novembre 2022

DELL Technologies

Soddisfare le esigenze di tutte le organizzazioni.

Sviluppo della maturità Zero Trust.

Il framework definito Zero Trust e la serie di principi che ne sono alla base indicano le modalità ideali di gestione della sicurezza. È possibile implementare il framework ricorrendo a varie funzionalità. Dell è un partner di sicurezza esperto che ti supporta nell'avanzamento lungo il percorso di sicurezza, sia che tu decida per l'approccio Zero Trust completo sia che tu scelga di concentrarti su miglioramenti specifici, allineandoti ai principi Zero Trust.

- Settore chimico
- Informatica
- Comunicazioni
- Servizi di emergenza
- Prodotti alimentari e agricoltura
- Difesa
- Settore sanitario e salute pubblica
- Produzione
- Settore finanziario
- Reattori nucleari
- Settore commerciale
- Pubblica amministrazione
- Energia
- Trasporti
- Acqua e acque reflue
- Dighe

DELL Technologies

DELL Technologies

Partner esperto di tecnologia e sicurezza per il percorso Zero Trust della tua organizzazione.

Migliorare la sicurezza informatica a lungo termine implementando l'approccio Zero Trust.

Dell Security Services offre:

La valutazione della maturità della sicurezza e del rischio complessivo da parte di esperti.

Sviluppo di roadmap Zero Trust.

Gestione continua delle attività di sicurezza.

DELL Technologies

Dell.com/SecuritySolutions

Richiedi di essere contattato

Avvia una chat con un consulente per la sicurezza

Chiama il numero 1-800-433-2393