Fidati della tua sicurezza. Fidati dei tuoi dipendenti. Con Lenovo.

Come proteggere la tua forza lavoro in un ambiente di sicurezza informatica in continua evoluzione

Smarter technology for all

Lenovo

Il passaggio irrevocabile al lavoro ibrido ha creato un ambiente di sicurezza informatica complesso.

Oggi la maggior parte dei lavoratori deve essere predisposta per il lavoro ibrido. Di conseguenza, la protezione dalle minacce deve essere estesa a più cloud e a piattaforme diverse.

Questo crea un ambiente digitale complesso che può essere un luogo in cui si nascondono minacce sconosciute. L'applicazione dei criteri di sicurezza ai dispositivi e a diversi livelli digitali è un compito davvero arduo, un'attività che comporta notti insonni per gli addetti alla protezione.

Una partnership unica con hardware e cloud sicuri: Il risultato dell'esclusiva partnership tra Lenovo e Microsoft è la combinazione dell'hardware ThinkShield con i servizi Microsoft Cloud Security.

Sicurezza integrata sin dalla fase di progettazione con Lenovo ThinkShield

In Lenovo comprendiamo l'urgente necessità di una protezione completa. Riflettendo le best practice in materia di protezione, promuoviamo il nostro approccio alla sicurezza ThinkShield con l'obiettivo di aumentare la sicurezza del nostro portfolio di dispositivi sin dalla fase di progettazione.

Ciò avviene a partire dalla protezione delle catene di approvvigionamento fino allo sviluppo di nuovi prodotti Lenovo sicuri e progettati dai produttori dei PC aziendali più affidabili al mondo.

Il nostro esclusivo portfolio ThinkShield di hardware, servizi, software e processi offre protezione a tutti i livelli aziendali. Le nostre partnership con i provider di soluzioni di sicurezza leader del settore offrono incredibili sistemi di difesa che incapsulano, contengono e promuovono una strategia Zero-Trust, basata sulle soluzioni di sicurezza Microsoft.

Zero-Trust. Il futuro della protezione informatica. La forma di una nuova direzione.

L'approccio Zero-Trust rappresenta un importante svolta rispetto alla sicurezza di rete tradizionale con un "perimetro aziendale" o dispositivi connessi tramite una VPN, che oggi è la norma.

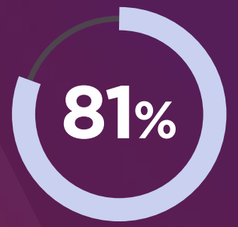
Zero-Trust si basa su un principio guida: "Non fidarti mai. Verifica sempre".

Nell'odierno ambiente di lavoro ibrido, i dispositivi non devono essere considerati affidabili a priori, anche se sono connessi a una rete "autorizzata".

Zero-Trust si basa sul presupposto della presenza di un utente malintenzionato all'interno della rete. L'attendibilità viene stabilita in base al **contesto**, ad esempio **l'identità e la posizione dell'utente, lo stato di sicurezza del dispositivo** e **l'app o il servizio richiesto**. Sono previsti controlli dei criteri in ogni passaggio.

Ciò garantisce che solo **le persone giuste con le risorse idonee su dispositivi sicuri possano accedere ai tuoi dati**.

La necessità di implementare un approccio Zero-Trust non è mai stata così urgente:



delle imprese ha avviato il passaggio al lavoro ibrido[1]

di riduzione del rischio di violazione dei dati[3]

1.070%
di aumento di ransomware tra luglio 2020 e giugno 2021[4]

delle organizzazioni riferisce di aver rilevato un attacco di phishing negli ultimi 18 mesi[2]

di riduzione delle chiamate effettuate agli analisti di help desk e IT[3]

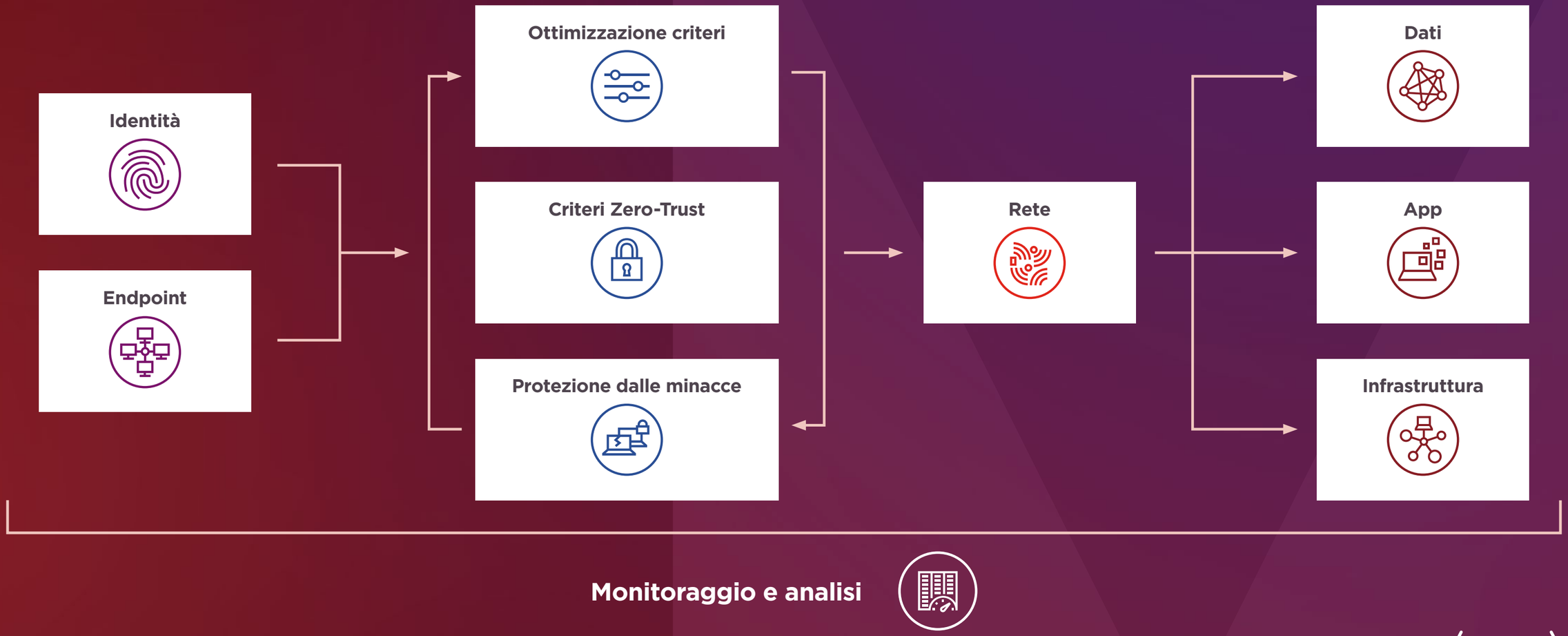
di riduzione dei tempi di gestione grazie al miglioramento dei processi di sicurezza[3]

Il portfolio Lenovo ThinkShield e le soluzioni Microsoft Security sono progettati in modo specifico e mirato per aiutarti a implementare una strategia Zero-Trust end-to-end e proteggere la tua azienda a tutti i livelli.

[1] Microsoft Zero Trust Adoption Report, 2021
[2] IBM Cost of a Data Breach Report 2021
[3] The Total Economic Impact™ of Zero Trust solutions from Microsoft, dicembre 2021. Studio di Forrester Consulting, commissionato da Microsoft.
[4] 11H Global Threat Landscape Report di FortiGuard Labs

Ecco l’aspetto dell’architettura Zero-Trust.

Il concetto di Zero-Trust è diffuso in molte parti dell’IT, ma la protezione inizia con i dispositivi moderni Windows 11, le identità degli utenti e il monitoraggio dei dispositivi endpoint.



Migliora e proteggi l’esperienza di lavoro ibrida per i tuoi dipendenti con i dispositivi Lenovo Windows 11 Pro

Windows 11 Pro, la versione di Windows più sicura di sempre, ti aiuta a **semplificare la gestione** del tuo ambiente di lavoro ibrido mentre **proteggi i dati e accedi** ovunque.

Progettato per i dispositivi moderni ottimizzati per la sicurezza, offre i vantaggi della **protezione basata su hardware** più avanzata, strettamente integrata con il software. Windows 11 Pro è progettato appositamente per il **lavoro ibrido sicuro** con uno **standard di sicurezza più elevato rispetto a Windows 10**, tra cui nuovi requisiti per la protezione, integrati e abilitati per impostazione predefinita.

ThinkPad X1 Carbon

Migliora la sicurezza del tuo dispositivo Lenovo ThinkShield con Windows 11 Pro grazie alla gestione del cloud

La protezione delle identità e dei dispositivi endpoint è il primo passaggio fondamentale della definizione di una strategia Zero-Trust. Le identità e i dispositivi sono le due aree che rappresentano gli obiettivi principali di ladri di credenziali, e-mail di phishing, ransomware, altri tipi di malware e minacce avanzate.

Combina i dispositivi Lenovo Windows 11 con le soluzioni di sicurezza Microsoft Cloud per implementare una strategia Zero-Trust.

Gestione delle identità

- Abilita l'autenticazione a più fattori (MFA) che può bloccare il 99,9% degli attacchi di identità.
- Fornisce un motore dei criteri "intelligente" per l'accesso condizionale che consente di impostare regole specifiche per l'"accesso" dell'utente. In combinazione con l'autenticazione a più fattori, garantisce un equilibrio ottimale tra sicurezza e produttività dell'utente.

Gestione degli endpoint

- Assicurati che le app siano conformi ai protocolli di sicurezza della tua azienda utilizzando Mobile Access Management (MAM).
- Assicurati che i dispositivi siano conformi ai protocolli di sicurezza della tua azienda utilizzando Mobile Device Management (MDM) sui dispositivi di proprietà dell'azienda o BYOD.

Controlla, proteggi e gestisci sfruttando i vantaggi delle soluzioni di sicurezza nel cloud

Gestione delle identità con Azure Active Directory

- Azure Active Directory è un servizio di gestione delle identità e degli accessi basato sul cloud semplice ed efficiente che fornisce l'autenticazione a più fattori e l'accesso condizionale.
- Combina servizi di directory di base, gestione dell'accesso alle applicazioni e protezione dell'identità in un'unica soluzione.
- Aiuta i tuoi dipendenti ad accedere in modo sicuro alle risorse esterne, ad esempio Microsoft 365, il portale di Azure e migliaia di altre applicazioni SaaS.
- Protegge le risorse interne, ad esempio una intranet e le app cloud sviluppate dalla tua organizzazione.

Microsoft Defender per endpoint

Questa soluzione di sicurezza degli endpoint basata sul cloud leader di settore:

- Aiuta a proteggere da ransomware, malware senza file e altri attacchi sofisticati su Windows, Mac OS, Linux, Android e iOS.
- Individua le minacce nascoste monitorando continuamente e in tempo reale il comportamento del codice e le tecniche degli utenti malintenzionati, consentendo un rilevamento e una risposta rapidi.
- Risposta agli eventi e risoluzione automatizzate 24 ore su 24, 7 giorni su 7: aiuta i team di sicurezza a passare immediatamente dagli avvisi alla risoluzione basata su intelligenza artificiale.
- Servizio di ricerca delle minacce gestito da esperti Microsoft "su richiesta".

Microsoft Endpoint Manager

Ottieni la gestione e la sicurezza dei dispositivi endpoint in una piattaforma di gestione unificata:

- Protegge, distribuisce e gestisce tutti gli utenti, le app e i dispositivi endpoint senza interrompere i processi di lavoro esistenti.
- Aiuta a ottenere un ambiente di lavoro moderno e una gestione moderna per mantenere i dati al sicuro, nel cloud e in locale.
- Combina i servizi che potresti conoscere e che stai già utilizzando, tra cui Microsoft Intune, Configuration Manager, Desktop Analytics, co-gestione e Windows Autopilot.

Il dispositivo ideale, nel posto e al momento giusti con la soluzione di distribuzione Lenovo Zero-Touch

Una tecnologia moderna e sicura è la chiave per garantire il successo di qualsiasi azienda. Ma il tradizionale approccio manuale alla distribuzione è complesso, richiede molto tempo ed è soggetto a errori.

Ora esiste un modo più semplice per garantire che i tuoi dipendenti che lavorano in modalità ibrida e da remoto siano operativi: **la distribuzione di Lenovo Zero-Touch tramite Autopilot**.

Stimolerà il lavoro ibrido, aumenterà la produttività e consentirà ai team IT di concentrarsi sull'innovazione per promuovere la crescita del business.

Con **Windows Autopilot** i reparti IT non devono più riformattare tramite immagine o configurare nuovi dispositivi manualmente. Tutto viene eseguito da remoto. I dispositivi Lenovo con Windows 11 sono dotati di Autopilot preconfigurato. I responsabili IT possono personalizzare le configurazioni degli utenti e applicarle ovunque si trovino.

- **Dispositivi pronti all'uso immediatamente:** sarà sufficiente accendere il dispositivo e con pochi semplici clic l'utente sarà pronto per il suo business.
- **Semplice gestione dei profili:** puoi creare, gestire e assegnare fino a 350 profili diversi per definire le impostazioni di un utente e la relativa esperienza con il PC.
- **Transizione al cloud senza problemi:** aggiungi automaticamente i dispositivi ad Azure Active Directory e registrali nella gestione dei dispositivi mobili.
- **Provisioning senza problemi:** configurazione personalizzata e semplificata.
- **Monitoraggio dello stato di avanzamento:** con Autopilot gli utenti possono monitorare lo stato della configurazione del dispositivo.
- **Registrazione del prodotto:** i dispositivi vengono registrati automaticamente al servizio di distribuzione cloud Autopilot.

Adotta un approccio di tipo “L’unione fa la forza”.

Sicurezza immediata

- **Protezione profonda** con la sicurezza hardware TPM 2.0 e soluzioni di protezione di dati e identità.
- Accesso più semplice e sicuro utilizzando metodi di **autenticazione senza password** come Windows Hello for Business.
- Blocco del software dannoso con **la protezione integrata già abilitata**.
- Per garantire una **protezione fin dall’inizio**, Windows 11 impedisce il caricamento del malware all’avvio.
- Protezione di dati e rete supportata da **un’affidabilità basata su hardware** che aiuta a mantenere e verificare l’integrità del dispositivo.

Protezione dalle minacce in continua evoluzione

- Proteggi le credenziali con la **protezione antiphishing avanzata** in Microsoft Defender SmartScreen.
- Accedi a mani libere con il **rilevamento della presenza** che consente di eseguire l’accesso quando ti avvicini e applica il blocco quando ti allontani.
- Proteggi i tuoi dati più sensibili con i PC con **protezione a livello di core di Lenovo**.
- Ottieni la protezione delle credenziali basata su hardware con **Microsoft Pluton**.
- Approfitta del **rilevamento intelligente delle minacce e delle risposte rapide** basate su 43 trilioni di segnali di sicurezza analizzati quotidianamente.
- La crittografia BitLocker aiuta a **proteggere le informazioni aziendali**, anche su dispositivi smarriti o rubati.
- Ottieni maggiore **protezione da origini non attendibili**: apri file e siti Web in un contenitore isolato con Microsoft Defender Application Guard.

Gestione della sicurezza moderna

- **Mantieni aggiornate le funzioni di sicurezza** con Windows Update per le aziende.
- Abilita l’adozione di framework di **sicurezza Zero-Trust**.
- **Garantisci la conformità ai criteri per i dipendenti in sede e da remoto** con Microsoft Endpoint Manager.
- Distribuisci dispositivi **preconfigurati con criteri di sicurezza** aziendali utilizzando Windows Autopilot e la distribuzione zero-touch.
- Ottieni sicurezza e visibilità abilitando **il Single Sign-On sicuro** in tutte le tue app con Azure Active Directory.
- **La progettazione cloud-first consente una facile estendibilità** con Microsoft 365, Microsoft Defender per il cloud e Microsoft Defender per gli endpoint.
- Aiuta a prevenire il **codice dannoso** e proteggiti da malware e altri software non attendibili con Windows Defender Application Control.

Lenovo: il tuo partner di fiducia per l’implementazione della strategia Zero-Trust e il lavoro ibrido

Perché scegliere Lenovo?

Esperienza, competenza, funzionalità di livello enterprise e un team dedicato di esperti per supportare l’adozione del cloud, la definizione dei criteri di sicurezza e le implementazioni.
In qualità di partner autorizzato Microsoft Cloud Solutions Provider (CSP), Lenovo offre il portfolio completo di servizi Microsoft Cloud, inclusi i servizi Microsoft 365 e Azure.

Microsoft Partner

Microsoft

2022 Partner of the Year Winner
Device Award

Microsoft Gold Partner e Device Partner dell'anno

Lenovo soddisfa i severi requisiti di Microsoft per il riconoscimento come Gold Partner, il che conferma che Lenovo ha l'esperienza e le capacità per fornirti soluzioni di fascia alta e sicure per il tuo lavoro da remoto.

Inoltre, Lenovo ha ricevuto il prestigioso premio come partner dell'anno di Microsoft Device, come riconoscimento di eccellenza nella creazione, nella commercializzazione o nella vendita di dispositivi e soluzioni IT che promuovono la tecnologia basata su Microsoft.

Il premio è arrivato a seguito della comprovata esperienza di Lenovo nel fornire soluzioni e servizi integrati in modo coerente, flessibile e prevedibile, al fine di soddisfare l'attuale domanda di digital transformation dei clienti e rendere le loro attività a prova di futuro.

La nostra strategia cloud: tutto da un unico fornitore

L'obiettivo di Lenovo è quello di diventare una vera organizzazione ibrida, in grado di distribuire cloud in locale, privato e pubblico soddisfacendo le esigenze dei clienti in termini di storage, software e soluzioni. Tutto ciò si collega alla nostra capacità di offrire hardware, servizi, software, modelli Device-as-a-Service e supporto, tutto da un unico fornitore.

Ecco come garantiamo il funzionamento della soluzione strategica Zero-Trust per la tua azienda

I servizi gestiti e professionali Lenovo possono consentirti di passare senza problemi alle difese Zero-Trust.

- Dalla progettazione della soluzione all'onboarding fino alla migrazione finale, Lenovo ti offre supporto completo per ogni tua esigenza.
- Se disponi di una licenza Microsoft 365, aggiorniamo semplicemente i dispositivi Windows 11 e Microsoft 365 e includiamo Azure Active Directory, Microsoft Defender ed Endpoint Manager.
- Premier Support: linea telefonica dedicata agli utenti, 24 ore su 24, 7 giorni su 7, 365 giorni all'anno.
- Esperti dedicati: esperti locali pronti a supportare il tuo passaggio a un lavoro ibrido sicuro.
- Sicurezza di livello enterprise: le migliori difese per la sicurezza informatica che proteggono dalla crescente ondata di malware e di attacchi mirati.

Smarter technology for all

Lenovo

Contattaci oggi stesso per scoprire come Lenovo può supportarti nella creazione della strategia di sicurezza Zero-Trust della tua organizzazione.

Fissa un appuntamento

Microsoft 365