



AUMENTA LA SICUREZZA ZERO TRUST E COLMA LE LACUNE DELLA SICUREZZA IT

Perché l'adozione di un approccio zero trust può contribuire a proteggere il tuo ambiente di cloud ibrido

Inizia ora →

Sommario

**3 Criminalità informatica:
una minaccia globale**

**4 Verificare l'integrità e
convalidare l'approccio
alla sicurezza**

**5 Stabilire un approccio
orientato al business**

**6 Una spinta globale verso
l'adozione del modello
zero trust**

**7 Riscuotere successo con
un framework zero trust**

**8 Abilitare un framework
zero trust efficiente**

**9 È tutto pronto per
adottare l'approccio zero
trust?**

**10 Collabora con HPE per
adottare l'approccio zero
trust**

Criminalità informatica: una minaccia globale

Prepararsi di fronte a un inevitabile attacco informatico

Poiché il furto di informazioni digitali è diventato una minaccia globale diffusa, la sicurezza informatica ha guadagnato il centro della scena. Le agenzie governative, la pubblica amministrazione e il settore privato sono tutti bersagli delle minacce informatiche, inclusi ransomware, phishing, fuga di dati, violazioni e minacce interne.

Di conseguenza, per qualsiasi organizzazione che opera in qualunque settore, la domanda da porsi non è se si diventerà il bersaglio della criminalità informatica, ma quando avverrà l'attacco e quali saranno le sue conseguenze.

Considerando queste minacce, le organizzazioni hanno iniziato a concentrarsi maggiormente su strategie zero trust per cui nulla è attendibile, indipendentemente dal fatto che si tratti di utenti, dispositivi, sistemi, dati o applicazioni, finché non ne viene completata l'autenticazione e l'autorizzazione. Ulteriori fattori trainanti degli ambienti zero trust includono la volontà di fornire una connettività ibrida più sicura e flessibile per la forza lavoro sempre più mobile.

Hewlett Packard Enterprise può aiutarti a progettare e implementare una strategia e un'architettura zero trust che segua il principio di base secondo cui a nessun utente, dispositivo o carico di lavoro viene concesso l'accesso all'IT finché non viene identificato e solo dopo aver assegnato i privilegi di accesso appropriati.

Zero trust in cifre

64%

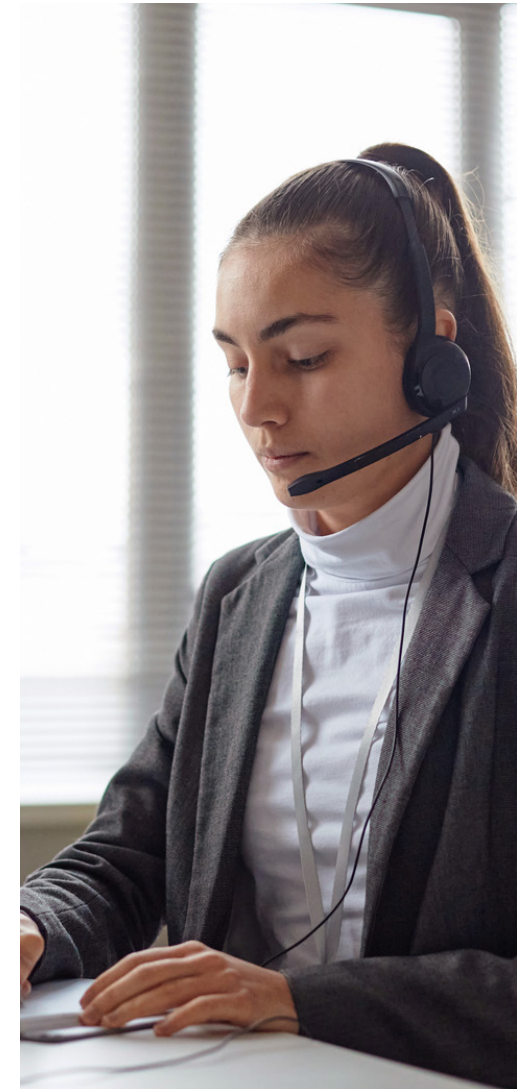
la probabilità che i team di sicurezza più performanti adottino modelli zero trust.¹

Entro il 2025

il 60% di tutte le organizzazioni adotterà modelli zero trust per la propria sicurezza.²

43%

percentuale delle organizzazioni ad alte prestazioni che hanno implementato o implementeranno un modello di sicurezza SASE.³



¹ [The 2022 Study on Closing the IT Security Gap: Global](#), studio del Ponemon Institute sponsorizzato da HPE, gennaio 2022

² [Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23](#), Gartner, giugno 2022

³ [The State of SD-WAN, SASE, and Zero Trust Security Architectures](#), studio del Ponemon Institute sponsorizzato da Aruba, aprile 2021



Verificare l'integrità e convalidare l'approccio alla sicurezza

Presupporre che ogni identità sia illecita finché non viene dimostrato il contrario

Tradizionalmente, le organizzazioni si sono affidate a un approccio "castello e fossato" alla sicurezza perimetrale,⁴ dove l'unico modo per attraversare il fossato e raggiungere il castello (il data center) è varcare un ponte (il firewall). Questo approccio presenta uno svantaggio significativo: presuppone che tutto all'interno del perimetro sia sicuro e non tiene conto degli attacchi interni.

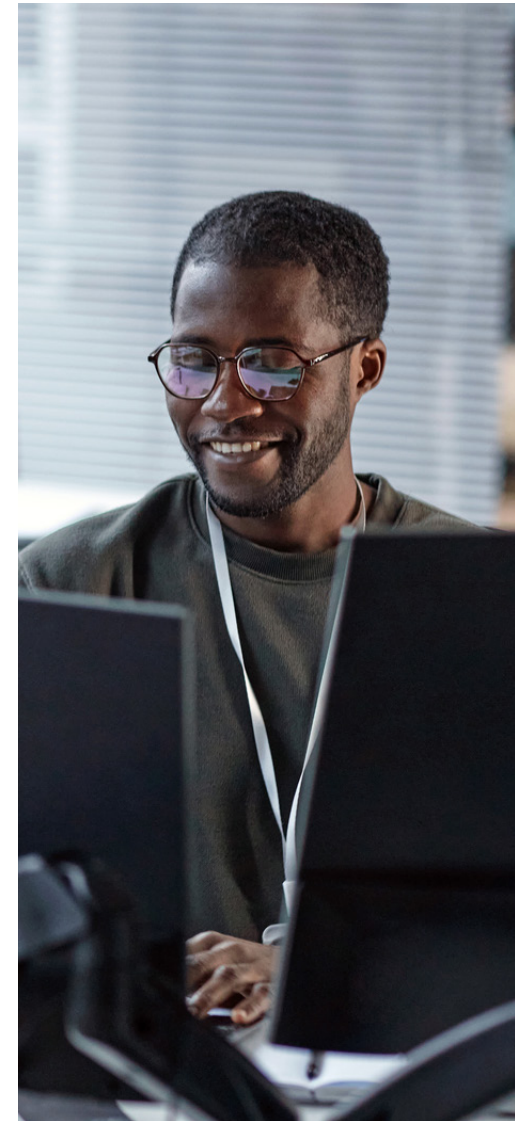
I Firewall, da soli, non sono più sufficienti per proteggersi dal panorama delle minacce in evoluzione e in espansione. Per garantire la massima sicurezza, oggi si deve presupporre l'assenza di un perimetro. Sono necessari nuovi metodi per proteggersi dalle intrusioni di minacce interne, malware e ransomware, nonché da minacce più avanzate e persistenti rivolte ai livelli inferiori dell'infrastruttura, inclusi bootkit e rootkit.

Di recente, tuttavia, le strategie di sicurezza sono state progettate intorno ai concetti di "attendibilità verificata" o zero trust. Questo approccio si basa sull'assunto che nulla è attendibile, per impostazione predefinita, e che è sempre necessario verificare le identità e presumere che l'entità possa introdurre una vulnerabilità di sicurezza, salvo prova contraria. Quando nulla è considerato attendibile per impostazione predefinita, ogni identità viene controllata e i privilegi di accesso all'ambiente IT vengono concessi soltanto dopo la verifica

dell'integrità basata sul contesto e adeguata al rischio. In breve, si presuppone che ogni identità sia illecita finché non viene dimostrato il contrario.

HPE può aiutarti a progettare e implementare una strategia zero trust dall'interno verso l'esterno, con la creazione di un'architettura tecnologica che verifica sempre tutto senza mai fidarsi di niente, conservando anche un registro completo degli eventi. HPE può aiutarti a implementare un modello zero trust dall'edge al cloud con HPE GreenLake, basandoti su architetture di riferimento e competenze per permettere alla tua organizzazione di sfruttare l'automazione e tutti i vantaggi del cloud ibrido.

Nulla è attendibile, per impostazione predefinita; verifica sempre le identità e presumi che l'entità possa introdurre una vulnerabilità di sicurezza, salvo prova contraria.



⁴ [What Is Perimeter Security In Cybersecurity](#), Security Forward, gennaio 2022



Stabilire un approccio orientato al business

Comprendere meglio perché la tua organizzazione vuole o deve adottare un approccio zero trust

Adottare un approccio zero trust orientato al business significa fare un passo indietro da un punto di vista tecnologico e comprendere meglio i motivi per cui la tua organizzazione vuole o deve adottare un modello zero trust. HPE può indicarti la giusta direzione da imboccare identificando il livello desiderato per il tuo panorama di sicurezza informatica, dove ti trovi oggi e il modo migliore per colmare il divario. Utilizzando queste informazioni, HPE può fornire una chiara visione dei punti in cui il modello zero trust è in grado di aggiungere valore alla tua organizzazione, nonché evidenziare come può consentirti di conseguire vantaggi in tempi rapidi e supportare casi d'uso aziendali.

Affinché un approccio zero trust a livello aziendale abbia successo, deve soddisfare sei principi chiave:

- attendibilità delle reti
- attendibilità delle infrastrutture
- attendibilità delle applicazioni
- attendibilità dei dispositivi
- attendibilità delle identità
- attendibilità dei dati

Andando al di là dell'opinione tradizionale secondo cui il modello zero trust viene applicato solo a livello

di rete, HPE espande il concetto per affermare che lo zero trust deve includere anche l'infrastruttura, le applicazioni e i carichi di lavoro definendo e applicando criteri di gestione delle policy e delle identità.

Dopo aver determinato una visione completa dell'ambiente attuale, esaminando i processi aziendali, l'inventario degli asset correnti, i controlli di sicurezza, l'architettura, il modello di governance della sicurezza, la strategia di sicurezza IT e qualsiasi iniziativa di crescita e di business futura, HPE personalizza la strategia zero trust affinché possa contribuire a proteggere la tua organizzazione, aiutando al tempo stesso la tua azienda ad adottare un approccio alla crescita basato sul rischio, reso possibile dalla sicurezza.

Pilastri chiave di una strategia zero trust:

- predisposizione per il futuro
- consapevolezza dei rischi
- flessibilità
- progettazione consolidata
- integrazione



Una spinta globale verso l'adozione del modello zero trust

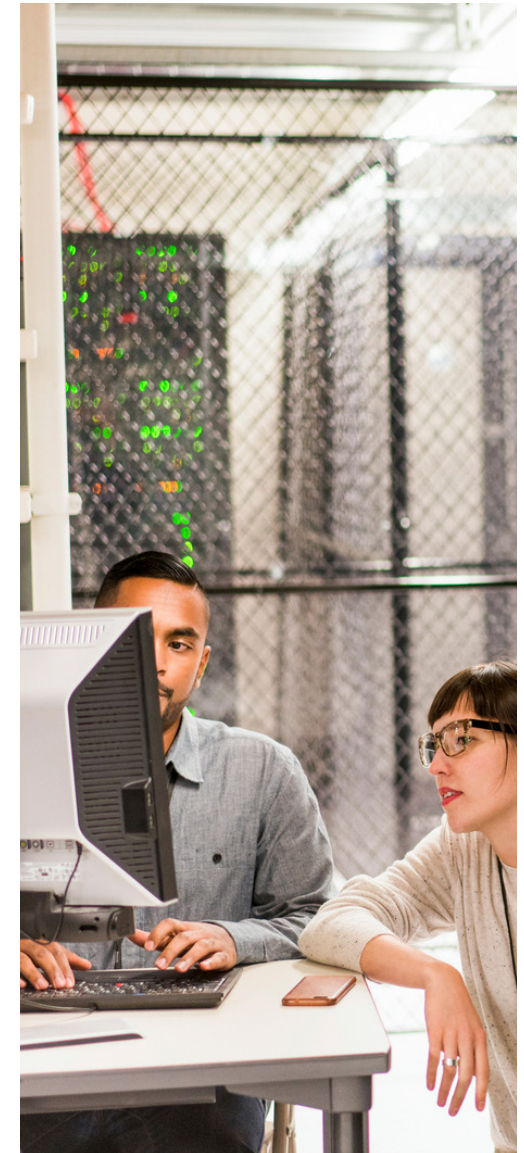
Comprendere le linee guida dei provvedimenti legislativi del governo degli Stati Uniti per migliorare l'approccio alla sicurezza informatica nel mondo zur Verbesserung des weltweiten Cybersicherheitsstatus

Nel maggio 2021, il governo degli Stati Uniti ha emanato un provvedimento legislativo per migliorare l'approccio alla sicurezza informatica della nazione.⁵ Il provvedimento contiene una serie di linee guida su come contrastare al meglio le attività informatiche dannose, persistenti e sempre più sofisticate che minacciano la pubblica amministrazione, il settore privato e, nel complesso, la sicurezza e la privacy delle persone in tutto il mondo. Queste linee guida includono dettagli su come le aziende possono migliorare le proprie iniziative per identificare, sventare, proteggere, rilevare e rispondere ad azioni dannose e utenti malintenzionati. Il provvedimento richiede inoltre alle agenzie e alle organizzazioni di:

- adottare best practice di sicurezza
- progredire verso l'adozione del modello zero trust
- accelerare le strategie di protezione dei servizi cloud, inclusi Software-as-a-Service, Infrastructure as-a-Service e Platform-as-a-Service
- centralizzare e semplificare l'accesso ai dati sulla sicurezza informatica per promuovere l'analisi in modo da identificare e gestire i rischi per la sicurezza informatica
- investire in tecnologia e personale per raggiungere questi obiettivi di modernizzazione

Il provvedimento ha spinto le imprese negli Stati Uniti e in tutto il mondo a considerare il modello zero trust come l'approccio preferito per migliorare la sicurezza informatica globale e risolvere le problematiche legate a costi per i danni causati all'economia dalla criminalità informatica, che si prevede raggiungeranno 10,5 trilioni di dollari all'anno a livello globale entro il 2025.⁶

Le nuove linee guida includono dettagli su come le aziende possono migliorare le proprie iniziative per identificare, sventare, proteggere, rilevare e rispondere ad azioni dannose e utenti malintenzionati.



⁵ [Executive Order on Improving the Nation's Cybersecurity](#), Casa Bianca, maggio 2021

⁶ [Cybercrime To Cost The World \\$10.5 Trillion Annually By 2025](#), Cybercrime Magazine, novembre 2020



Riscuotere successo con un framework zero trust

Far fronte alla mancanza di competenze interne e supportare l'infrastruttura per implementare il modello zero trust

HPE considera l'approccio zero trust in modo diverso rispetto ad altri fornitori. Riteniamo che il modello zero trust faccia sicuramente parte della struttura della rete, ma che vada applicato ugualmente a tutto il resto dello stack tecnologico, inclusi dati, applicazioni, persone, infrastruttura e sistemi operativi. In breve, HPE può fornire uno stack IT già predisposto per l'approccio zero trust. I nostri esperti di sicurezza possono contribuire a progettare e assegnare policy zero trust a ogni livello dello stack tecnologico per sfruttarne i vantaggi in tutta l'azienda, dall'edge al cloud.

Il successo di un framework zero trust inizia dall'adozione di un approccio orientato al business. Di conseguenza, è necessario acquisire una chiara comprensione dei motivi per cui la tua organizzazione deve adottare il modello zero trust e successivamente identificare il livello desiderato per il tuo panorama di sicurezza informatica, dove ti trovi oggi e il modo migliore per colmare il divario.

L'approccio orientato al business richiede anche la cooperazione tra i team di sicurezza e aziendali. Se il team di sicurezza conosce e comprende le operazioni del team aziendale, può progettare un'architettura di sicurezza che consenta all'azienda di raggiungere con successo i propri obiettivi.

Il primo passo in un'iniziativa zero trust orientata al business è definire il business case, partendo dalla comprensione di quali parti dell'ambiente IT saranno più appropriate per l'adozione del modello zero trust. Il passaggio successivo consiste nell'identificare alcuni casi d'uso per dimostrare l'approccio zero trust al resto dell'organizzazione.

L'adozione del modello zero trust può offrire importanti vantaggi aziendali e finanziari:



Rischi organizzativi ridotti



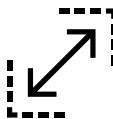
Probabilità di violazione della sicurezza ridotte



Controllo ottimizzato dello stack di sicurezza



Qualità superiore degli avvisi di sicurezza



Esperienza utente ottimizzata



Abilitare un framework zero trust efficiente

Progettare un framework zero trust esclusivo, basato su ogni singola organizzazione e sui suoi obiettivi di sicurezza

Ogni strategia zero trust progettata da HPE, sebbene sia unica nel suo genere, interagisce con il piano di controllo che include la governance della sicurezza, l'orchestrazione e tutte le altre funzionalità integrate in un'organizzazione. Inoltre, ogni strategia e architettura zero trust di HPE adotta un approccio specifico per reti, infrastrutture e carichi di lavoro, contribuendo a garantire la verifica di identità e integrità come elementi chiave. Senza l'automazione, fornita da HPE, l'implementazione di un modello zero trust può diventare molto più complessa.

Rete

Le iniziative per l'ambiente di lavoro ibrido, inclusi IoT ed edge computing, dissolvono il perimetro IT tradizionale. L'obiettivo delle organizzazioni è garantire connettività sempre e ovunque senza sacrificare la sicurezza, conservando visibilità e controllo senza influire sull'esperienza dell'utente. HPE può aiutarti a raggiungere questo obiettivo con il [controllo accesso di rete Aruba ClearPass](#) e [Aruba ClearPass Policy Manager](#).

Infrastruttura

HPE propone elementi costitutivi cloud native sicuri e predisposti per l'approccio zero trust con verifica dell'integrità attivata nella supply chain sicura e integrata nella Silicon Root of Trust, a partire dal momento della produzione in una supply chain sicura. Durante tutto il processo di produzione fino alla delivery, al primo avvio viene attivata una conferma basata su zero trust prima che qualsiasi elemento possa connettersi alla rete.

Carichi di lavoro

La soluzione per carichi di lavoro zero trust HPE sfrutta i progetti open source Secure Production Identity Framework for Everyone (SPIFFE) e SPIFFE Runtime Environment (SPIRE) della Cloud Native Computing Foundation. Questi progetti consentono ad HPE di applicare i principi zero trust ai propri servizi forniti in un ambiente cloud con implementazioni, inclusi sistemi HPC, data fabric end-to-end e piattaforma edge to cloud. Con l'approccio zero trust di HPE, ogni identità viene verificata continuamente, per garantire che due organizzazioni reciproche possano collaborare utilizzando identità attendibili. Questo livello di convalida zero trust è possibile solo tramite il monitoraggio continuo.

Con HPE, puoi:

- identificare e risolvere le lacune di sicurezza con la combinazione ideale di progettazione di sicurezza integrata e monitoraggio costante
- ridurre i costi e l'impatto sul brand della criminalità informatica identificando e resolvendo in modo proattivo le minacce e consentendo al personale IT e di sicurezza di concentrarsi sulle priorità aziendali
- colmare le lacune nelle competenze di sicurezza con la consulenza degli esperti di HPE



È tutto pronto per adottare l'approccio zero trust?

Blocca gli attacchi informatici prima che si verifichino

L'adozione di un approccio zero trust orientato al business aggiunge valore a tutti i livelli della tua organizzazione. Con la combinazione ideale di progettazione di sicurezza integrata e monitoraggio costante, la tua organizzazione può ridurre i costi e l'impatto sul brand della criminalità informatica identificando e risolvendo in modo proattivo le minacce e consentendo al personale IT e di sicurezza di concentrarsi sulle priorità aziendali. HPE può aiutarti a:

- verificare che la sicurezza sia progettata nei casi d'uso aziendali dall'edge al cloud
- ridurre i rischi organizzativi attraverso una comprensione più approfondita del tuo ambiente
- migliorare significativamente il controllo sul tuo stack di sicurezza
- ridurre i costi CAPEX e OPEX
- rendere la sicurezza trasparente agli utenti
- ridurre l'ambito della conformità tramite il monitoraggio e l'ispezione continui del tuo ambiente

Con i **servizi HPE Managed IT Compliance**, gli esperti HPE possono supportarti nell'identificazione e nella risoluzione delle lacune di sicurezza con la combinazione ideale di progettazione di sicurezza integrata.. Scopri tutte le novità sulle normative e sui controlli di conformità, in costante evoluzione, necessari per proteggere e ottimizzare i rischi per la sicurezza e la conformità nel tuo ambiente multicloud mentre adotti e ottimizzi il tuo approccio zero trust.





Visit [HPE.com](https://www.hpe.com)

Collabora con HPE per adottare l'approccio zero trust

Di fronte a un inevitabile attacco informatico, un approccio zero trust orientato al business può aiutarti a bloccarlo prima che si verifichi. Scopri come HPE può contribuire a farti ottenere visibilità completa, controllo granulare e applicazione con una base integrata per zero trust progettata per tutelare i dati riducendo al contempo i rischi, colmando le lacune di competenze e risorse e abbattendo i costi operativi.

Ulteriori informazioni alla pagina

Contatta il tuo rappresentante HPE oggi stesso per saperne di più sull'adozione di un approccio zero trust orientato al business. Scopri come la tua organizzazione può:

- ottenere visibilità completa, controllo granulare e applicazione con una base integrata per i framework Zero Trust e SASE: [Aruba ClearPass Policy Manager](#)
- proteggere i dati e attenuare i rischi con [HPE Managed IT Compliance](#), fornito come servizio gestito

[Chatta ora \(commerciale\)](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i servizi e i prodotti Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni ed errori tecnici o editoriali contenuti nel presente documento.

a50007343ITE,, Rev. 2

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

