



Adotta un approccio zero trust e colma le lacune nella sicurezza IT

HPE utilizza un approccio zero trust per costruire architetture sicure per il mondo edge to cloud di oggi



Un approccio del tipo “non fidarti di nulla, verifica sempre tutto” può proteggere il tuo ambiente di cloud ibrido, dall’edge al cloud. Con la combinazione ideale di progettazione della sicurezza integrata e monitoraggio costante di utenti, dispositivi, sistemi, dati e applicazioni, puoi migliorare il tuo livello di sicurezza e prevenire i cyberattacchi prima che influiscano negativamente sulla tua organizzazione.

Criminalità informatica: una minaccia globale

Il furto di informazioni digitali è ormai una minaccia globale e pervasiva. Le agenzie e le aziende sono i bersagli ideali di ransomware, phishing e hacking.

Si prevede che i costi associati ai crimini informatici a livello globale cresceranno del

15% l’anno

nei prossimi 5 anni, raggiungendo i 10,5 trilioni di dollari l’anno entro il 2025.¹

Entro il 2031 si stima che il ransomware costerà all’economia mondiale

265 miliardi di dollari.²

Nella prima metà del 2021 abbiamo assistito a un

aumento del 102%

nei reati informatici che coinvolgono il ransomware.³

L’89%

delle organizzazioni ospita dati sensibili nel cloud, sollecitando l’esigenza di una mentalità edge to cloud zero trust.⁴

Ogni organizzazione è alle prese con la stessa domanda di base: come possiamo proteggere i nostri asset e dati proprietari da questi attacchi continui? Come possiamo individuare gli elementi non affidabili prima che diventino un problema? Le aziende sono alla ricerca di approcci nuovi e olistici per proteggere le proprie risorse digitali, dall’edge al cloud, e con il contributo di Hewlett Packard Enterprise.

HPE può aiutarti a progettare e implementare una strategia zero trust basata su un’architettura in grado di supportare questo tipo di framework con automazione, applicazione di policy ed esperienza, per garantire che a nessun utente, dispositivo o carico di lavoro venga concesso l’accesso all’IT della tua organizzazione prima che sia stato identificato e gli siano stati assegnati i privilegi di accesso appropriati.

Lo sapevi?

Il 64%

dei team di sicurezza in grado di raggiungere le massime prestazioni adatteranno con tutta probabilità modelli zero trust.⁵

Il 60%

di tutte le organizzazioni adatterà modelli zero trust per la propria sicurezza entro il 2025.⁶

Il 78%

dei team di sicurezza in grado di raggiungere le massime prestazioni è più consapevole dei vantaggi dell’automazione, soprattutto per quanto riguarda l’identificazione degli attacchi prima che causino danni o diventino persistenti.⁷

Il 71%

dei team di sicurezza in grado di raggiungere le massime prestazioni è più consapevole dell’assoluta necessità dell’automazione per implementare un modello di sicurezza zero trust efficace.⁸

Zero trust

è sia un principio di sicurezza che una visione organizzativa.⁹

E dunque, come si fa a fidarsi di ciò che non è affidabile? HPE può aiutare la tua azienda ad adottare un framework zero trust e a creare un ambiente sicuro flessibile, scalabile e automatizzato.

L’adozione di un approccio zero trust data-driven in tutta la tua organizzazione fornirà:



Protezione dei dati e riduzione del rischio organizzativo



Verifica dell’integrità automatizzata e continua



Visibilità completa e migliore controllo del tuo ambiente distribuito



Controllo granulare delle regole e delle policy di accesso ai dati

Insieme a HPE GreenLake, puoi adottare l’approccio zero trust per proteggere i tuoi dati nel mondo edge-to-cloud di oggi.

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 in che modo la tua organizzazione può:

- Ottenere visibilità completa, controllo granulare e applicazione con una base integrata per i framework zero trust e SASE con [HPE Aruba ClearPass Policy Manager](#).
- Proteggere i dati e attenuare i rischi con [HPE Managed IT Compliance](#), fornito come servizio gestito.

¹ “Cybercrime To Cost The World \$10.5 Trillion Annually By 2025”, Cybercrime Magazine, novembre 2020

² “Global Ransomware Damage Costs Predicted To Exceed \$265 Billion By 2031”, Cybercrime Magazine, giugno 2022

³ “The New Ransomware Threat: Triple Extortion”, Check Point Blog, maggio 2021

⁴ “Sensitive Data in the Cloud”, Cloud Security Alliance, luglio 2022

^{5,7,8} “The 2022 Study on Closing the IT Security Gap: Global”, studio del Ponemon Institute sponsorizzato da HPE, gennaio 2022

^{6,9} “Gartner unveils the Top Eight Cybersecurity Predictions for 2022-23”, comunicato stampa Gartner, giugno 2022

Visit [HPE.com](#)

[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 prodotti e i servizi Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento può essere interpretato come garanzia aggiuntiva. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni o errori tecnici o editoriali contenuti nel presente documento.

a50007373ITE, Rev. 2

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

