



La sicurezza parte dalla rete

Protezione basata sull'AI integrata nella rete, non aggiunta a posteriori



La rete non è più un'infrastruttura che resta sullo sfondo. Costituisce invece il fondamento digitale da cui la tua azienda dipende per operare, innovare e crescere. Per la sua importanza, è diventata uno degli obiettivi più interessanti per i malintenzionati.

Le minacce si evolvono di giorno in giorno. La forza lavoro è ovunque, i dispositivi si moltiplicano e i dati sono continuamente in movimento. Il perimetro che un tempo separava l'ambiente "interno" da quello "esterno" si è dissolto e il personale IT deve trovare il modo di proteggere tutto senza rallentare il business né ridurre la produttività.

Le reti del passato non sono state progettate per affrontare le minacce di oggi

La sicurezza perimetrale e le combinazioni casuali di tool puntuali non avevano lo scopo di gestire i livelli di scala, velocità e sofisticatezza attuali. Alle aziende serve un approccio radicalmente diverso: una rete in cui la sicurezza zero trust è integrata per progettazione in ogni singola connessione, non aggiunta a posteriori.

Quando sicurezza e networking convergono, la rete diventa un motore di protezione strategico che rafforza le difese, semplifica le operazioni e accelera la generazione dei risultati di business.

Perché questo cambiamento si sta verificando proprio adesso?

- **Le superfici di attacco delle reti si stanno espandendo:** ogni singolo dispositivo, utente, sede e carico di lavoro aggiunge un nuovo punto di ingresso potenziale.
- **La pressione per la compliance è in aumento:** le normative attuali impongono un'applicazione continua e coerente, cosa difficile da garantire con i tool legacy.
- **La proliferazione degli strumenti introduce nuove lacune:** i sistemi disconnessi ostacolano il rilevamento, impedendo di fermare tempestivamente gli attacchi.
- **Il business non può rallentare:** le reti devono rimanere efficienti, resilienti e sicure anche sotto pressione.

La tua rete si sta trasformando in una soluzione di sicurezza

Ma in cosa consiste la sicurezza integrata nella rete?

Tutto parte da una rete che poggia su un fondamento sicuro, in cui le funzionalità di protezione sono integrate per progettazione fin dall'inizio, e non aggiunte in un momento successivo. Con questo approccio, la sicurezza diventa una componente naturale delle operazioni di rete, semplificando l'applicazione coerente della protezione da parte dei team, senza interferire con le prestazioni né interrompere i flussi di lavoro.

La protezione integrata supporta l'accesso sicuro da qualsiasi luogo tramite un'architettura predisposta per SASE, che fornisce una combinazione di networking e sicurezza per i moderni ambienti distribuiti. I principi zero trust possono essere attivati per tutti gli utenti, i dispositivi e le sedi tramite controlli basati sull'identità che seguono il soggetto ovunque si connetta.

Le operazioni basate sull'AI rafforzano ulteriormente questo approccio, analizzando continuamente comportamenti e rischi, rilevando tempestivamente le anomalie e fornendo raccomandazioni automatizzate sulle policy o sulle opzioni di risposta a disposizione dei team. In questo modo si ottiene una rete caratterizzata da una sicurezza intrinseca, più semplice da utilizzare, più adattabile e più allineata con le attuali modalità di gestione della connettività negli ambienti aziendali.

Prerequisiti per la sicurezza integrata

Questa base predispose le reti in modo che possano svolgere un ruolo più attivo, allo scopo di:

- **Proteggere tutti i domini in modo coerente:** gli ambienti edge, cloud e IoT, così come gli utenti remoti, sono tutti protetti da controlli unificati.
- **Applicare i principi zero trust ovunque, non solo in posizioni discrete:** le decisioni di accesso sono precise e vengono applicate in tempo reale, eliminando anche i colli di bottiglia creati dalle VPN.
- **Vedere di più per rilevare di più:** la visibilità basata sull'AI rivela le minacce nascoste prima che si trasformino in incidenti.
- **Semplificare senza scendere a compromessi:** la gestione unificata e l'utilizzo di un singolo motore di policy riducono la proliferazione dei tool e i costi generali.
- **Rafforzare compliance e governance:** i controlli integrati promuovono in modo più affidabile il rispetto dei requisiti di legge.
- **Garantire resilienza anche sotto pressione:** le reti AI-native semplificano l'isolamento dei problemi e garantiscono la continuità dei servizi.
- **Allineare i team di rete e sicurezza:** le informazioni condivise e i flussi di lavoro unificati eliminano i silos e rafforzano le misure difensive.

Protezione senza complessità

La rete AI-native sicura di HPE unifica SD-WAN, SSE, NAC cloud-native e firewall mesh ibrido per supportare lo ZTNA universale e offrire una sicurezza con efficacia leader di settore in tutti gli ambienti. Anziché cercare di combinare tool diversi, puoi beneficiare di un'architettura edge-to-cloud appositamente realizzata per garantire sicurezza zero trust e protezione avanzata.

Le informazioni basate sull'AI e la correzione automatica offrono ai team i livelli di velocità e sicurezza necessari per supportare nuove applicazioni, espandere i servizi e proteggere quello che conta di più.

HPE fa la differenza

- ✓ Una vera piattaforma SASE single vendor: SD-WAN sicura, SSE cloud-native e NAC basato sull'AI
- ✓ ZTNA universale con accesso sia tramite agente che in modalità agentless
- ✓ Prestazioni di sicurezza di altissimo livello: da oltre 5 anni siamo al 1° posto nei test indipendenti¹
- ✓ Profilazione basata sull'AI per una visibilità continua su qualunque infrastruttura
- ✓ Integrazioni con un ampio ecosistema di provider di soluzioni di sicurezza indipendenti
- ✓ Risoluzione dei problemi e rilevamento delle anomalie intelligenti e automatizzati



¹ HPE Juniper Networking SRX was ranked #1 in performance in the following research and testing programs: NetSecOPEN (2022), CyberRatings.org (2024 Cloud Network Firewall, 2025 Enterprise Firewall)

Connessione affidabile per una protezione continua

La rete AI-native sicura di HPE offre alla tua azienda tutta l'agilità di cui ha bisogno per innovare senza introdurre rischi inutili. La protezione zero trust integrata, la gestione unificata e la risposta automatizzata alle minacce garantiscono una protezione coerente, a prescindere da come si evolve l'ambiente. Mentre l'azienda si espande, la rete si adatta garantendo prestazioni resilienti e una sicurezza più efficace, ovunque lavorino dipendenti e collaboratori.

Ulteriori informazioni alla pagina

[HPE.com/networking](https://hpe.com/networking)



Visita [HPE.com](https://hpe.com)

[Avvia chat](#)

© Copyright 2026 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 esplicite 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 o errori tecnici o editoriali contenuti nel presente documento.

a00156866ITE

HEWLETT PACKARD ENTERPRISE

hpe.com

