

I sintomi che indicano che il firewall legacy non è adatto a supportare lo zero trust

Il lavoro moderno può svolgersi ovunque: in ufficio, in aereo, a casa o in fabbrica. Ora che le applicazioni sono ospitate sul cloud o utilizzate direttamente come servizio SaaS, Internet è diventata la nuova rete aziendale. **Il firewall legacy è davvero efficiente per proteggere utenti, dati e applicazioni con un approccio zero trust?** Se è presente uno dei seguenti sintomi, potrebbe essere giunto il momento di fare un check-up.

SINTOMO N. 1

Nessun rilevamento del movimento laterale

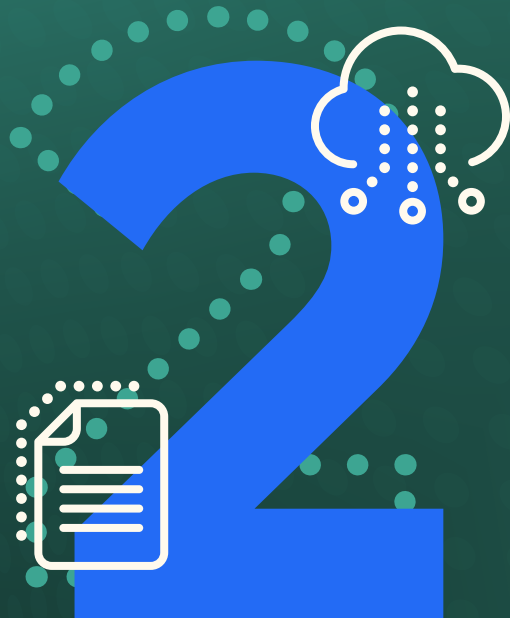
Quando gli utenti operavano dagli uffici e le applicazioni si trovavano esclusivamente su data center protetti da firewall tradizionali, l'attendibilità era implicita. Tuttavia, se un aggressore riesce a infiltrarsi sulla rete compromettendo un utente o sfruttando un errore di configurazione, bloccare l'accesso in tempo reale per arrestare il movimento laterale risulta praticamente impossibile.



SINTOMO N. 2

Le risorse cloud sono a rischio

I firewall virtuali vengono eseguiti sotto forma di istanze di VM sul cloud pubblico, il che richiede la distribuzione di un'istanza in ogni punto di ingresso e di uscita. Dato che i firewall tradizionali sono stati progettati per proteggere il perimetro della rete aziendale, gli aggressori possono sfruttare agevolmente i punti deboli del cloud per compromettere l'integrità e la sicurezza di workload e dati sensibili.



SINTOMO N. 3

Dipendenza da policy permissive (temporanee o dimenticate)

Gli sviluppatori agili desiderano innovare più velocemente e, spesso, chiedono agli amministratori IT e della sicurezza policy altamente permissive, almeno temporaneamente, per accelerare i progetti. Capita però che queste policy vengano dimenticate. I firewall tradizionali faticano ad applicare modifiche dinamiche alle policy in base ad attributi comportamentali e ambientali osservabili.



L'85% degli amministratori di rete ritiene che le funzionalità del firewall vengano fornite in modo migliore attraverso il cloud.¹

Scopri tutti i 7 sintomi che indicano che i firewall legacy e next-gen non sono adatti a supportare lo zero trust e perché è necessario implementare un firewall nativo del cloud.

[Scarica l'e-book](#)

1. Fonte: Zscaler, Indagine sui firewall di rete