SCHEDA TECNICA

Zscaler Microsegmentation

Sfide con la microsegmentazione legacy

Molte aziende si affidano ad architetture di segmentazione legacy per proteggere i propri workload. Queste architetture si rivelano inadeguate perché sono complesse da implementare, aumentano la superficie di attacco, amplificano il movimento laterale e incrementano i costi operativi.

- Ottenere un inventario accurato delle risorse è difficile, in particolare per quelle nel cloud, che vengono caricate e scaricate dinamicamente.
- Le soluzioni come i firewall estendono la rete a workload e server amplificando i rischi di movimento laterale.
- L'insieme di dispositivi virtuali, strumenti operativi e policy non standard introduce problemi noti e ignoti nella copertura di sicurezza, aumentando il rischio.
- Gli strumenti di segmentazione personalizzati di terze parti sono complessi da implementare, e l'applicazione delle policy di sicurezza aziendali è incoerente.

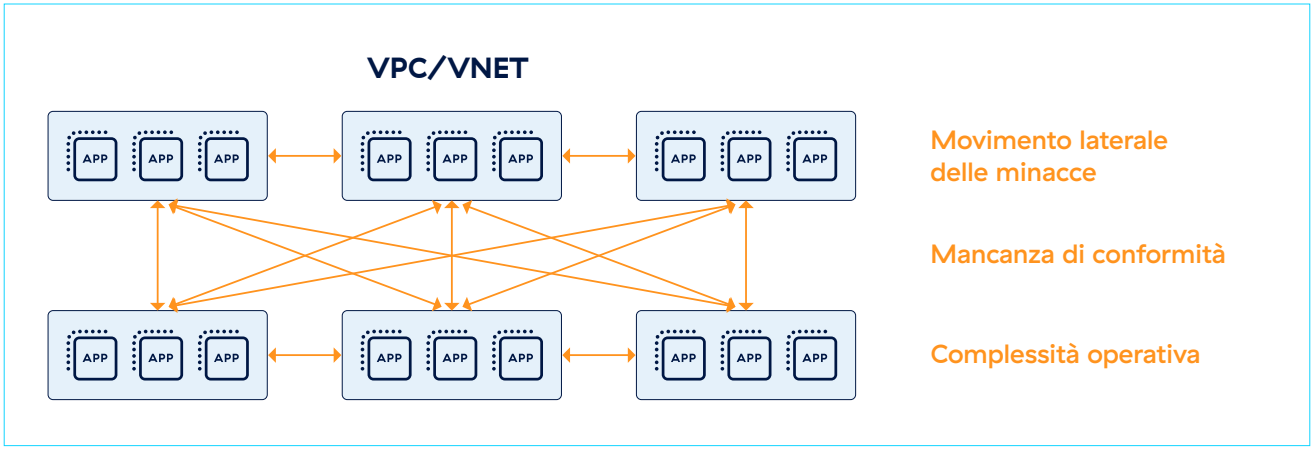

Figura 1: le architetture legacy di protezione dei workload sono inadeguate per fermare il movimento laterale delle minacce

Estendi l'architettura zero trust per segmentare i workload nei cloud pubblici e nei data center on-premise

La microsegmentazione basata su host affronta queste sfide suddividendo la rete in segmenti più piccoli e controllabili. Le regole di sicurezza vengono applicate a ciascun segmento, concedendo solo l'accesso essenziale. In questo modo, se un segmento viene violato, il resto della rete rimane sicuro. Con l'avanzare delle minacce informatiche, è evidente che le difese basate sul perimetro non riescono più a fermare gli attacchi sofisticati.

Zscaler Microsegmentation fornisce:

Rilevamento e visibilità delle risorse in tempo reale: ottieni l'inventario delle risorse in tutta la tua infrastruttura.

- Scopri le risorse quasi in tempo reale. Ottieni un inventario delle risorse in base a tag definiti dall'utente, attributi cloud (VPC/VNET) e oggetti di rete (IP/subnet).
- Ottieni visibilità sulle risorse presenti su più cloud pubblici, data center e co-location in un'unica console.

Suggerimenti automatizzati sulle policy: assicurati che tutte le risorse siano coperte da una policy di sicurezza.

- Ricevi suggerimenti sulle policy per segmentare i flussi di lavoro in base all'analisi del flusso di traffico.
- Ricevi suggerimenti proattivi sulle policy, in modo da coprire le risorse non segmentate.

Applicazione granulare delle policy: ferma il movimento laterale delle minacce.

- Applica controlli a livello host per limitare l'accesso.
- Ottieni una policy di sicurezza uniforme per tutte le risorse nei data center e nel cloud pubblico.

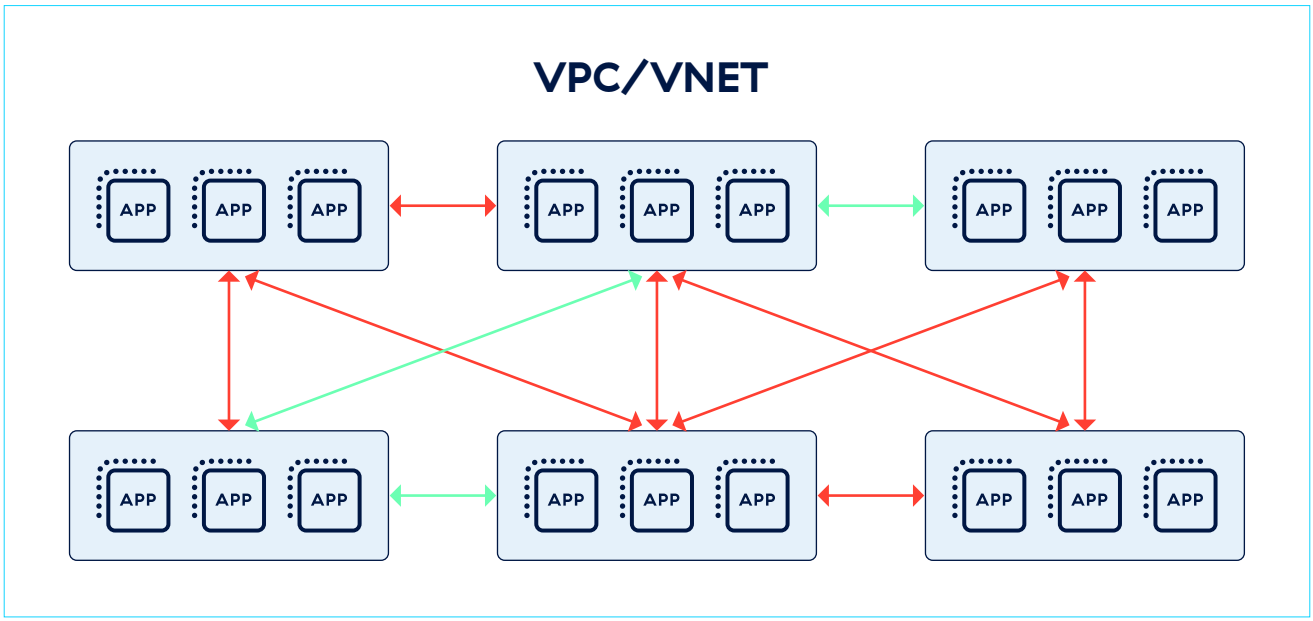

Figura 2: Zscaler Microsegmentation offre una segmentazione basata sull'host e sullo zero trust

Funzionalità di Zscaler Microsegmentation

Funzionalità	Dettagli
Copertura del cloud pubblico e on-premise	Proteggi i workload in AWS e Microsoft Azure con un supporto aggiuntivo per i server dei data center on-premise.
Inventario host	Ottieni visibilità sui tuoi workload cloud, con i dettagli su host, ambiente cloud e tag definiti dall'utente.
Inventario di flusso	Ottieni visibilità granulare sui flussi, inclusi i dettagli sull'IP e le porte sia di origine che di destinazione, il protocollo, il nome e il percorso dell'applicazione.
Mappa delle applicazioni	Ottieni una mappa interattiva dei flussi corrispondenti tra le risorse applicative nell'ambiente.
Policy sulle risorse	Crea e applica policy tra le risorse della tua applicazione.
Zone di applicazione	Controllo delle regole delle policy in base alle zone o agli ambienti applicativi.
Aggiornamenti semplificati degli agenti	Aggiorna gli agenti di Zscaler Microsegmentation per gruppi utilizzando i profili di versione.
Dashboard di analisi	Le dashboard di analisi includono le risorse più importanti come iniziatori, destinatari e flussi verso Internet in base ai log di flusso osservati.
Ampio supporto della piattaforma	Gli agenti leggeri possono essere installati sui sistemi operativi più comuni, tra cui Windows e Linux.
Streaming dei log	Consolida i log di tutti i workload e server a livello globale in un repository centrale definito dalla tua organizzazione con Zscaler Log Streaming Service. Gli amministratori possono visualizzare ed estrarre i dati del registro del traffico dai workload in tempo reale.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/it