aruba
a Hewlett Packard Enterprise company

SFRUTTA IL POTENZIALE DI SASE:

una rete più sicura dall'edge al cloud

Il lavoro da remoto ha accelerato la transizione al cloud.
Come si possono migliorare le prestazioni di rete e colmare le lacune di sicurezza?
Come deve cambiare l'architettura dell'ambiente?

Il 53% dei nuovi dipendenti da remoto vuole continuare a lavorare da remoto

Cloud, edge e IoT stanno ridefinendo il posizionamento di dati e applicazioni

Abilitando un'architettura SASE per integrare rete e sicurezza, è possibile proteggere più efficacemente l'azienda

Un'infrastruttura di rete e sicurezza organizzata in silo non è più sostenibile

Il numero delle applicazioni aziendali implementate nel cloud continua ad aumentare

Oggi, utenti e dispositivi non sono più confinati nel tradizionale perimetro dell'azienda

Perché gli approcci tradizionali a rete e sicurezza non funzionano più

Problemi legati alla presenza di silo isolati di rete e sicurezza e all'uso di un approccio limitato incentrato sull'hardware:

- Aumento dei livelli di complessità accompagnato da una diminuzione di flessibilità ed efficienza
- Riduzione della resilienza e dell'efficacia del disaster recovery
- Perdita di opportunità e rischio di farsi superare dalla concorrenza
- Difficoltà a soddisfare i requisiti per l'uso del cloud e il supporto degli utenti che lavorano a domicilio

Perché è necessario un edge zero trust

Una soluzione edge zero trust assicura autenticazione avanzata, controllo degli accessi in base al ruolo e all'identità, oltre a una segmentazione appropriata di utenti e dispositivi fra data center, edge e cloud.

Integrando SASE con un framework di policy di gestione delle identità zero trust e basate su ruoli, è possibile proteggere utenti, dispositivi, dati e applicazioni, dall'edge al cloud.

Forrester 2021

Vantaggi di un edge zero trust e di SASE

- Integrazione della sicurezza nel DNA della rete
- Assegnazione di priorità al traffico generato dalle applicazioni aziendali predominanti nella rete WAN delle filiali
- Protezione delle aziende da clienti, dipendenti, collaboratori esterni e dispositivi che si connettono tramite fabric WAN ad ambienti caratterizzati da un livello di rischio superiore
- Accesso sicuro ai servizi e alle applicazioni aziendali per proteggere i dipendenti da remoto
- Protezione e segmentazione di utenti e dispositivi IoT in base ai requisiti aziendali
- Supporto della gestione centralizzata, del monitoraggio e dell'analisi di tutti i servizi di rete e sicurezza che risiedono all'interno delle soluzioni edge zero trust

È necessario intraprendere un percorso verso l'edge zero trust? Ecco 3 domande da porre all'azienda

1. Qual è il livello di sicurezza delle applicazioni aziendali nel cloud?
2. Come si possono proteggere i dispositivi e gli utenti all'edge?
3. Il 53% dei lavoratori vuole continuare a lavorare da remoto. L'azienda è pronta?

PRESENTAZIONE DEL MODELLO EDGE ZERO TRUST PER I SERVIZI DI RETE E SICUREZZA:

Un Secure Access Services Edge (SASE) è un edge zero trust

Leggi il report di Forrester per scoprire:

- perché le operazioni e le infrastrutture di rete e sicurezza organizzate in silo stanno rapidamente scomparendo
- il metodo edge zero trust più adatto a un'azienda specifica
- come valutare le opzioni multi vendor e single vendor

Leggi il report

aruba
a Hewlett Packard Enterprise company