CHECKLIST

6 consigli fondamentali per migliorare la produttività degli utenti e la sicurezza del perimetro di rete

Le imprese accelerano le loro iniziative di trasformazione digitale, puntando a rendere più intuitiva, efficace e rapida l'interazione degli utenti con le applicazioni, grazie alle moderne tecnologie di rete, multi-cloud e SaaS. L'accelerazione digitale avvicina le applicazioni e i dati agli utenti e ai dispositivi, ma è ostacolata dalle reti legacy, che forniscono accesso implicito a tutte le applicazioni.

Le reti tradizionali non sono progettate per rispondere alle esigenze attuali del lavoro da qualsiasi luogo e degli ambienti multi-cloud/SaaS. Oltre a frenare l'accelerazione digitale, peggiorano l'esperienza degli utenti e creano problemi di sicurezza. Le organizzazioni devono abilitare la zero-trust implicita per tutte le applicazioni. In che modo si può migliorare la produttività e allo stesso tempo la sicurezza del perimetro di rete?

☑ 1. Investire in tecnologie di rete moderne

Le organizzazioni devono investire in tecnologie di rete moderne. SD-WAN e LTE/5G migliorano la connettività WAN, offrendo agli utenti un'esperienza migliore grazie all'accesso diretto a Internet. LAN e WLAN forniscono un accesso più rapido ai dispositivi e agli utenti locali.

☑ 2. Distribuire rete e sicurezza in modo unificato e convergente

La sicurezza non può essere aggiunta a posteriori. Quando le soluzioni di sicurezza non sono ben integrate tra di loro o con la rete sottostante, l'espansione e l'evoluzione della superficie di attacco porta con sé rischi e lacune di sicurezza. Si creano punti ciechi, vulnerabili a sofisticati attacchi in più fasi, e questo è uno dei motivi del preoccupante aumento degli attacchi ransomware portati a segno. Per questo è importante affidarsi a soluzioni SD-WAN, 5G, LAN e WLAN dove la sicurezza è integrata e non un'aggiunta forzosa.

Le organizzazioni necessitano di un framework di sicurezza unificato per garantire una sicurezza automatizzata e reattiva che copra l'intera superficie di attacco. Devono inoltre supportare la convergenza unificata di sicurezza e rete per proteggere l'accelerazione digitale.

☑ 3. Combinare la strategia Zero Trust Edge con una gestione unificata di sicurezza e rete

Con la moltiplicazione dei perimetri di rete negli ambienti locali e cloud, è fondamentale rendere disponibile ovunque la convergenza unificata di funzionalità di rete e sicurezza insieme allo ZTNA, per abilitare l'accesso esplicito alle applicazioni e la verifica continua di utenti e dispositivi. Questa convergenza è il cuore di una strategia Zero Trust Edge. È inoltre fondamentale che questa convergenza sia implementata in modo flessibile, per proteggere l'accelerazione digitale nelle distribuzioni ibride.

☑ 4. Velocizzare le operazioni con una gestione centralizzata e automatizzata

La crescita esponenziale di strumenti, perimetri di rete e piattaforme cloud può aumentare significativamente la complessità operativa. Inoltre, la scarsa visibilità e le lacune analitiche della rete, unite allo svolgimento manuale dei compiti, deteriorano l'esperienza digitale complessiva.

Questi problemi causano un aumento dei tempi di configurazione, gestione e risoluzione dei problemi. Aumentano inoltre i costi di gestione e gli errori che possono causare interruzioni della rete e ridurre la flessibilità. Adottando una gestione centralizzata e automatizzata e un'unica dashboard per l'intero stack di rete e di sicurezza, si accelera la fornitura dei servizi di rete durante il loro intero ciclo di vita. L'eliminazione delle operazioni di configurazione manuale rimuove una delle cause principali dei tempi di inattività e delle violazioni della sicurezza.

☑ 5. Aumentare la visibilità con il monitoraggio completo dell'esperienza digitale

Il monitoraggio tradizionale delle prestazioni della rete, dell'infrastruttura IT e delle applicazioni offre ai team NOC una visibilità limitata. Questi tipi di monitoraggio non forniscono le informazioni sulle prestazioni delle applicazioni aziendali critiche di cui i clienti hanno bisogno. Inoltre, ostacolano gravemente la visibilità necessaria ai team NOC e dell'help desk in prima linea per risolvere i problemi.

Una moderna piattaforma di monitoraggio dell'esperienza digitale è necessaria per dare al team NOC una visibilità superiore, consentendo di osservare qualsiasi applicazione, a partire dall'utente finale, attraverso qualsiasi rete, fino all'infrastruttura dove l'applicazione è ospitata. Può fornire strumenti aggiuntivi per gestire gli incidenti e un rimedio olistico ai problemi di prestazioni.

☑ 6. Unificare e semplificare le operazioni per fornire un ROI immediato

Le organizzazioni che adottano le tecnologie di rete moderne con sicurezza integrata ottengono un ROI migliore rispetto ai prodotti monofunzionali con limitate capacità di sicurezza. Aumentano inoltre la produttività dei dipendenti migliorando la user experience e semplificando le operazioni.

Conclusioni

Molte organizzazioni utilizzano ancora un'architettura tradizionale per collegare gli uffici al data center per l'accesso alle applicazioni. Nel mondo moderno, tuttavia, in cui gli utenti lavorano da qualsiasi luogo e le applicazioni sono distribuite su ambienti multi-cloud/SaaS, questo design di rete è ormai obsoleto e ostacola l'accelerazione digitale, peggiorando l'esperienza degli utenti. Le organizzazioni che desiderano migliorare la produttività degli utenti e proteggere il perimetro aziendale devono investire in un'architettura di rete moderna.

Fortinet è l'unico fornitore del settore in grado di proteggere qualsiasi perimetro su qualsiasi scala e di integrare la sicurezza nelle moderne tecnologie di rete, come SD-WAN, 5G, wireless LAN e switching con un unico sistema operativo. Offrendo la migliore convergenza tra funzionalità di rete e sicurezza, Fortinet consente alle organizzazioni di adottare le moderne tecnologie di rete essenziali per l'accelerazione digitale. Il modello Zero Trust Edge di Forrester convalida l'approccio alla convergenza di Fortinet.

FORTINET®

www.fortinet.com

maggio 23, 2022 12:33 PM
1457355-0-0-IT