citrix

Lista di controllo

Sette aspetti fondamentali per fornire un accesso remoto sicuro

Anche se mantenere i sistemi sicuri non è mai stata un'operazione facile, quando tutti si recavano in ufficio per lavorare era di certo più semplice. Attualmente, i dipendenti distribuiti lavorano su una varietà di reti non protette dal reparto IT e su dispositivi che la tua organizzazione potrebbe non gestire. In questo contesto è più difficile ottenere visibilità sulle azioni potenzialmente rischiose che i dipendenti possono intraprendere e su come tali azioni possono influire sulla sicurezza dei dati aziendali.

Al contempo, è essenziale riconoscere che le applicazioni e i dati non risiedono più solo all'interno dei datacenter aziendali, ma sono distribuiti su vari servizi cloud e in locale. Inoltre, anche le applicazioni aziendali critiche vengono distribuite dal cloud.

Ma poiché facciamo sempre più affidamento sul cloud, la tua esposizione agli attacchi sta aumentando e il numero di minacce per la sicurezza sta crescendo rapidamente. La tua superficie di attacco ora contempla vari fattori tra cui dispositivi, applicazioni, file e reti che i dipendenti remoti utilizzano per svolgere il proprio lavoro. Anche se ciascuno di questi fattori è fondamentale ai fini

1. Zero Trust Network Access (ZTNA) per tutte le applicazioni autorizzate dal reparto IT

Grazie alla flessibilità aumenta l'adozione da parte degli utenti e cresce l'efficienza, ma è importante garantire che la sicurezza protegga le applicazioni e i dati senza interferire con il modo in cui gli utenti svolgono il proprio lavoro.

Le soluzioni basate su appliance, come le VPN e gli SWG, sono state progettate in base a un principio che richiede di "fidarsi implicitamente" di qualcosa di noto. Sfortunatamente, il concetto di "fiducia implicita" (Implicit Trust) viene sfruttato da molti metodi di attacco moderni che utilizzano credenziali compromesse, inseriscono contenuti dannosi o utilizzano un dispositivo rubato o compromesso per accedere alle informazioni e rubare la proprietà intellettuale.

Lo Zero Trust va contro il principio di Implicit Trust e si concentra sul **"non fidarti, verifica sempre" (Never Trust, Always Verify)**.

Le soluzioni tradizionali si concentrano solo sull'autenticazione e sull'autorizzazione degli utenti al momento dell'accesso o sul blocco di URL sospetti solo una volta inseriti nella blacklist. Al contrario, lo Zero Trust presuppone che tutti gli utenti e gli URL siano sospetti, a meno che non dimostrino il contrario. Pertanto, lo Zero Trust consente di monitorare e valutare continuamente le attività degli utenti durante tutta la sessione e di automatizzare i controlli di sicurezza in base alle anomalie rilevate.
suspicious URLs only once they are blacklisted. In contrast, Zero Trust assumes all users and URLs are suspicious unless they prove otherwise. Zero Trust thus enables you to continuously monitor and assess user activities throughout the session and automate security controls based on anomalies detected.

Per adottare lo Zero Trust per proteggere le applicazioni e i dati, è necessario fornire sicurezza ai dipendenti remoti a livello di applicazione per prevenire gli attacchi a livello di rete, applicando al contempo il controllo contestuale degli accessi supportato da assessment continui. Ciò richiede la capacità di scansionare i dispositivi degli utenti finali prima e dopo l'attivazione di una sessione e di definire il modo in cui gli utenti vengono autenticati e autorizzati ad accedere alle loro applicazioni.

2. Esperienze eccezionali

Se gli utenti riscontrano un'esperienza IT insoddisfacente, andranno alla ricerca di soluzioni alternative che possono penalizzare la produttività e la sicurezza. Le soluzioni basate su appliance (come VPN e SWG) sono state progettate per una piccola percentuale di dipendenti remoti e forniscono sicurezza solo per un sottoinsieme di applicazioni. In un contesto in cui sempre più dipendenti adottano il lavoro mobile o remoto, le soluzioni basate su appliance sono difficili da adattare, richiedendo il backhauling del traffico e un'esperienza di accesso separata. Per prevenire questi problemi è fondamentale che il reparto IT fornisca una soluzione in grado di offrire la migliore esperienza utente e sicurezza possibili. Spesso, questo significa superare la VPN per adottare workspace più unificati che forniscono ai dipendenti gli strumenti giusti per lavorare ovunque.

3. Single sign-on (SSO) per tutte le applicazioni autorizzate dall'IT

Indipendentemente dall'utilizzo di dispositivi BYOD, aziendali, condivisi o desktop dedicati, la tua soluzione di accesso remoto dovrebbe semplificare l'esperienza utente. Funzionalità come il single sign-on (SSO) forniscono un accesso sicuro a desktop e applicazioni virtuali, ai repository di documenti e a tutte le applicazioni autorizzate dal reparto IT. Le soluzioni SSO inoltre semplificano l'accesso per gli utenti, in quanto non hanno bisogno di ricordare né gestire vari nomi utente e password. Inoltre, gli utenti possono avvalersi di una singola console per tutte le applicazioni e i file, riducendo al minimo il carico sul reparto IT per risolvere i problemi di password o ripristinare i privilegi di accesso scaduti.

4. Autenticazione adattiva e controlli del comportamento del dispositivo

L'autenticazione adattiva con assessment del comportamento del dispositivo dirige in modo intelligente l'utente al meccanismo di autenticazione più adatto in base al ruolo, alla posizione geografica e al controllo del comportamento del dispositivo. Ad esempio, a un collaboratore temporaneo su un dispositivo non identificato possono essere richieste ulteriori fasi di autenticazione, oppure a un dipendente che accede a un'applicazione da una posizione insolita può essere negato l'accesso.

L'accesso alle applicazioni può essere abilitato in base al ruolo utente, alla posizione e all'analisi del comportamento del dispositivo. Grazie all'assessment del comportamento del dispositivo, il reparto IT può analizzare gli endpoint in base a vari fattori, come antivirus, sistema operativo, firewall, registri e altro ancora.

5. Prestazioni delle applicazioni

Gli utenti che riscontrano prestazioni applicative insoddisfacenti nutrono frustrazioni e diventano improduttivi. Tuttavia, attraverso una tecnologia che aumenta la visibilità e il controllo delle prestazioni applicative, il reparto IT può ridurre le interruzioni e la latenza della rete e delle applicazioni. Ciò si traduce in un maggiore uptime, migliori SLA dell'helpdesk e minori probabilità che gli utenti aggirino i controlli di sicurezza per via delle scarse prestazioni applicative.

6. Rilevamento e difesa dai rischi potenziali in modo automatico

Gli analytics forniscono insight su applicazioni, file, dispositivi e reti; pertanto aiutano il reparto IT ad automatizzare le misure di sicurezza in base al comportamento degli utenti e alle anomalie rilevate. L'assessment continuo dei rischi e l'intervento adattivo aiutano il reparto IT a diminuire il lavoro manuale, a garantire un intervento tempestivo e a ridurre al minimo il rischio di violazioni non autorizzate.

Le soluzioni come la navigazione remota consentono al reparto IT di garantire che gli utenti finali possano navigare in modo sicuro sul web, senza introdurre rischi nell'ambiente aziendale. Questo ti protegge dalle minacce che possono essere introdotte da siti web dannosi garantendo che questi browser siano isolati fuori dalla rete e dai dispositivi aziendali.

7. Consolidamento IT e fusioni e acquisizioni

Il consolidamento della gestione di servizi, reti, cloud e applicazioni IT in una piattaforma unificata aiuta a ridurre la complessità IT, a migliorare la produttività dei dipendenti con una migliore esperienza dell'utente finale, a ridurre il costo totale di proprietà e a prevenire le lacune di sicurezza nell'infrastruttura che potrebbero aumentare i rischi di conformità.

Laddove le organizzazioni acquisiscono altre aziende, per il reparto IT è importantissimo integrare rapidamente i nuovi dipendenti e ridurre al minimo le interruzioni per consentire all'azienda di proseguire il suo percorso. Tuttavia, è difficile adattare le soluzioni basate su appliance poiché è possibile impiegare settimane per procurarle, installarle e renderle disponibili per l'uso per i nuovi dipendenti. Pertanto, è fondamentale che il reparto IT limiti l'accesso di questi utenti solo a determinate applicazioni e non fornisca l'accesso completo alla rete fino a quando non sia tutto pronto.

Conclusioni

Nel pianificare il modo in cui la modernizzazione dell'IT fornirà un ambiente sicuro e produttivo per la tua forza lavoro ibrida, hai bisogno di esplorare soluzioni completamente integrate, fornite come servizio cloud. Con una soluzione che prevede più fornitori è praticamente impossibile centralizzare la gestione e l'automazione della sicurezza. Sui prodotti con più fornitori non funziona nessuna delle policy di sicurezza e dei profili di rischio degli utenti, e questo costringe gli amministratori della sicurezza a eseguire processi manuali lenti.

Citrix Unified Secure Access offre una soluzione completamente unificata e pronta per la distribuzione che consente di massimizzare le prestazioni, minimizzare i rischi e aumentare la produttività della forza lavoro ovunque e su qualsiasi dispositivo.

citrix

Enterprise Sales
Nord America | 800 424 8749
In tutto il mondo | +1 408 790 8000

Sedi
Sede centrale | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, Stati Uniti
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, Stati Uniti