Symantec by Broadcom | Carbon Black. by Broadcom | Arrow

GUIDA

Guida pratica

Sicurezza e resilienza con Symantec ZTNA

La tua rete privata virtuale (Virtual Private Network, VPN) promette un accesso remoto sicuro, ma in realtà offre una porta aperta alla tua rete. Le VPN tradizionali danno per scontato che chiunque si trovi all'interno del perimetro della rete sia affidabile, e questo è un problema. Trasforma ogni appaltatore, partner e fornitore terzo in un potenziale vettore di violazione.

Quando gli aggressori compromettono le credenziali di un singolo appaltatore, non accedono solo a un'applicazione, ma possono muoversi liberamente nell'intera rete. Recenti violazioni di alto profilo hanno dimostrato che l'accesso di terze parti è diventato l'anello debole della sicurezza aziendale.

Symantec Zero Trust Network Access (ZTNA) cambia questa equazione, sostituendo la fiducia cieca con una verifica continua e un accesso a tutta la rete con connessioni precise specifiche per ogni applicazione.

Perché è il momento di affrontare la crisi dell'accesso di terze parti

Le VPN tradizionali sono progettate per garantire l'accesso completo alla rete, poiché non sono in grado di prevedere quali applicazioni saranno necessarie agli utenti. Questo approccio "tutto o niente" implica che un lavoratore remoto, un consulente o un appaltatore incaricato di aggiornare il tuo sito Web possa potenzialmente accedere ai tuoi sistemi finanziari, ai database dei clienti e alla proprietà intellettuale. Le scansioni delle vulnerabilità e le tecniche di mappatura espongono l'intera topologia della rete a chiunque disponga di credenziali di base.

Una lacuna nella visibilità aggraverà ulteriormente questo rischio. I dati essenziali per la conformità e la risposta agli incidenti sono sparsi su più server, dispositivi e sedi in formati diversi. In questo modo i team di sicurezza si trovano in difficoltà nel reperire informazioni durante la risposta agli incidenti, perché le attività degli utenti si estendono su sistemi disconnessi. Non puoi difendere ciò che non puoi vedere.

L'accesso con dispositivi personali (Bring-your-own-device, BYOD) rappresenta un ulteriore problema. Spesso appaltatori e partner utilizzano i propri dispositivi. Le regole aziendali potrebbero non consentire a tali dispositivi di utilizzare la tua VPN oppure la tua VPN potrebbe non supportarli.

Infine, il supporto VPN implica l'implementazione di complesse configurazioni DMZ e regole firewall che assorbono le risorse IT. Inoltre, obbliga il traffico a passare attraverso i data center centrali, creando colli di bottiglia che ostacolano il lavoro da remoto.

Costruire la resilienza con ZTNA

Zero Trust capovolge le regole della sicurezza di rete. Invece di dare per scontato che tutti coloro che si trovano all'interno del perimetro siano affidabili, funziona secondo un principio semplice: mai fidarsi e verificare sempre.

Ogni richiesta di accesso è sottoposta a verifica in base a ZTNA. I sistemi valutano l'identità dell'utente, lo stato del dispositivo, la posizione, il metodo di autenticazione e persino l'URI specifico dell'applicazione in una richiesta di accesso.

Questo approccio al perimetro definito dal software si concentra sulla protezione delle singole applicazioni, nascondendole completamente agli utenti non autorizzati. Segue un modello di accesso "meno privilegiato" e consente l'accesso solo alle applicazioni per le quali l'utente ha l'autorizzazione.

Symantec ZTNA sostituisce l'ampio accesso alla rete con connessioni punto-punto, creando tunnel sicuri tra utenti specifici e applicazioni specifiche. **Ciò contribuisce a offrire tre vantaggi chiave:**

Prestazioni

La connettività punto-punto elimina i colli di bottiglia e riduce la latenza. I test di Symantec hanno dimostrato che gli utenti hanno ottenuto tempi di transazione più rapidi del 62% rispetto alle connessioni VPN tradizionali. E con Symantec ZTNA in esecuzione su Google Cloud, gli utenti possono aspettarsi prestazioni più rapide e una scalabilità migliorata per soddisfare tutte le esigenze.

Sicurezza

ZTNA limita il raggio di azione di una compromissione nascondendo all'utente le parti non autorizzate della rete. Se un aggressore compromette una credenziale, ottiene l'accesso a una sola applicazione e a nient'altro. Il movimento laterale diventa impossibile quando non c'è una rete in cui muoversi.

Resilienza

I sistemi Symantec utilizzano l'infrastruttura Google Cloud per offrire tre zone di disponibilità per punto di presenza e failover con un clic in tutte le regioni del mondo. Ciò lo mantiene operativo anche durante i disastri naturali.

Sicurezza e resilienza con Symantec ZTNA

La tua tabella di marcia a fasi per l'implementazione di ZTNA

L'implementazione di ZTNA non deve essere necessariamente dirompente. Symantec consiglia un approccio in tre fasi per sfruttare i vantaggi e offrire funzionalità non presenti in una VPN.

Fase 1: agli utenti remoti offrire l'accesso con privilegi minimi

Il modello di accesso con privilegi minimi di Symantec ZTNA consente a tutti di accedere solo alle applicazioni che hanno il permesso di utilizzare.

Queste applicazioni sono nascoste al resto della rete, impedendo l'accesso dannoso o involontario ad applicazioni e dati sensibili.

Inizia con la tua forza lavoro remota, inclusi i dipendenti che lavorano da casa, i team di vendita in viaggio e il personale dislocato che ha bisogno di un accesso sicuro alle applicazioni. Questi utenti rappresentano la più grande superficie di attacco e il più alto impatto sulla produttività. Abilita l'accesso basato su agenti per i dispositivi gestiti e l'accesso senza agente per gli scenari BYOD. Symantec ZTNA supporta applicazioni Web, SSH nativo per i team DevOps, RDP per il desktop remoto e TCP per le applicazioni legacy.

Una volta che i dipendenti avranno un accesso sicuro, estendi la stessa protezione a collaboratori, partner e fornitori. Questo approccio dimostra rapidamente il suo valore presso i tuoi utenti principali, affrontando al contempo i rischi di terze parti. È efficace anche per fusioni e acquisizioni, poiché durante il processo la nuova organizzazione potrebbe aver bisogno di accedere alle risorse della società madre.

La tua VPN esistente può continuare a funzionare durante questa transizione, eliminando le interruzioni mentre convalidi il modello Zero Trust.

Fase 2: migliorare i controlli di sicurezza aggiungendo protezione ai dati e contro le minacce

In questa fase vengono aggiunte la protezione ai dati e contro le minacce. Le VPN creano un punto cieco in termini di sicurezza. Non possono ispezionare il traffico per individuare minacce o applicare policy di protezione dei dati. Symantec ZTNA cambia completamente questa situazione. Ogni connessione ad applicazioni private è ora sottoposta allo stesso controllo di sicurezza di qualsiasi altro traffico. Symantec ZTNA si integra direttamente con Symantec Threat Intelligence Service, che analizza tutti i file alla ricerca di malware e contenuti dannosi, nonché con Web Isolation, che protegge automaticamente gli utenti da siti sconosciuti o sospetti.

Symantec ZTNA si sincronizza anche con Symantec Data Loss Prevention (DLP), pertanto qualsiasi policy DLP esistente può essere applicata al traffico ZTNA, garantendo l'applicazione delle stesse protezioni e restrizioni.

Fase 3: distribuire ZTNA all'intera organizzazione

In questa fase Symantec ZTNA viene distribuito all'intera organizzazione, non solo agli utenti remoti. Offre a tutti, compreso il personale in sede, un metodo più sicuro per accedere alle applicazioni e alle risorse.

Con Symantec ZTNA, le stesse regole di conformità che regolano l'accesso SaaS e Web ora proteggono le applicazioni interne. L'ispezione del traffico avviene nel cloud senza dover implementare proxy o backhaul tramite data center, garantendo una protezione costante indipendentemente dal fatto che gli utenti accedano alle risorse cloud o locali. Le policy a livello di applicazione garantiscono che tutti gli utenti vedano solo ciò a cui sono autorizzati ad accedere, mentre tutto il resto rimane nascosto e invisibile. Ogni tentativo di accesso genera registri di controllo centralizzati, offrendoti una visibilità che le VPN non avevano.

Inoltre, è possibile distribuire un singolo agente che gestisce ZTNA insieme agli strumenti Symantec esistenti, come Cloud SWG, Cloud Access Security Broke, DLP e Web Isolation. Ciò semplifica notevolmente l'implementazione e la gestione, poiché un unico agente può essere utilizzato per più casi d'uso diversi.

Non appena vedrai risultati positivi, sarai pronto a eliminare gradualmente la tua infrastruttura VPN. Non è un caso che l'80% dei progetti pilota si converta in acquisti.

Sicurezza e resilienza con Symantec ZTNA

Realizzare il vantaggio SSE per le imprese moderne

Il consolidamento elimina la proliferazione degli strumenti. L'unione di ZTNA con Cloud SWG e DLP/CASB nell'ambito del framework Security Service Edge (SSE) rafforza, semplifica e ottimizza le operazioni di sicurezza.

I clienti Symantec SWG dispongono già di una componente fondamentale di un framework Zero Trust. Ora possono integrarlo senza problemi con ZTNA, utilizzando lo stesso agente, la stessa console di gestione e lo stesso framework di policy.

I vantaggi operativi sono immediati:

Distribuisci rapidamente

Implementa il sistema in pochi minuti anziché in settimane.

Proteggi tutto

Il servizio Threat Intelligence e Remote Browser Isolation di Symantec sono compatibili con tutti i servizi, garantendo una protezione unificata contro malware e minacce emergenti.

Semplifica la gestione

Gestisci un unico stack di sicurezza anziché dover gestire più fornitori con interfacce, modelli di licenza e processi di supporto diversi.

Conclusione

L'implementazione di ZTNA è un modo efficace per eliminare il rischio di trasformazione. Non si tratta solo di risparmiare denaro (anche se ridurre la proliferazione dei venditori aiuta sicuramente il budget). Si tratta di creare un'architettura di sicurezza che si adatti alla tua attività, riducendone al contempo la complessità.

Le organizzazioni che si affidano a VPN "abbastanza buone" accettano rischi non necessari. Oggi esiste una tecnologia che elimina i movimenti laterali, protegge l'accesso di terze parti e migliora contemporaneamente l'esperienza e le prestazioni dell'utente.

La questione non è se implementare o meno Zero Trust Network Access, ma quanto velocemente è possibile farlo.