10 ELEMENTI del data center Zero Trust

Un vero data center Zero Trust mette al primo posto l'esperienza dell'utente finale.

Questo significa:

- *Accesso veloce, affidabile e scalabile*
- *Utenti e dispositivi protetti*
- *Applicazioni e carichi di lavoro che proteggono i dati*
- *Sicurezza che rende più agile il business*

10 VISIBILITÀ SU CIÒ CHE È INVISIBILE

Non puoi proteggere ciò che non vedi.

Ti serve una visibilità completa sull'intera rete e i suoi diversi ambienti, e su come ogni parte è protetta: dal client al carico di lavoro.

9 SEGMENTAZIONE IN PIÙ PUNTI

Un controllo punto per punto.

La segmentazione e il controllo granulari - a partire da utenti e dispositivi, fino ad app e carichi di lavoro - possono impedire accessi indesiderati e prevenire lacune nella difesa.

8 IDENTITÀ PER UTENTI, DISPOSITIVI E CARICHI DI LAVORO

L'identità non riguarda solo gli utenti...

ma anche i dispositivi e i carichi di lavoro. L'identità è costituita da più fattori che in ogni momento aiutano a individuare i rischi nella rete.

7 POLICY INTEGRATE SENZA LIMITAZIONI IN BASE AL LUOGO

Segui gli utenti, i dispositivi e le applicazioni ovunque vadano.

Utenti, applicazioni e carichi di lavoro sono sempre in movimento. Assicurati che le policy di sicurezza seguano ogni loro movimento per limitare i potenziali vettori di attacco.

6 CAPIRE GLI INTENTI DEL TRAFFICO DI RETE

Dove è diretto il traffico e cosa fa?

Dovresti sapere il più possibile su tutto il traffico di rete e la sua destinazione, incluso il traffico che non stai decifrando. Ma come? Inizia osservando gli indicatori e i comportamenti specifici del traffico.

5 AUTOMATIZZA OVUNQUE SIA POSSIBILE

Usa l'automazione come un superpotere.

Rende il tuo lavoro più semplice e migliora l'efficacia dei team. L'automazione può far sì che le modifiche apportate in una parte del data center vengano applicate ovunque e ti consente di rispondere agli attacchi prima che diventino veri incidenti.

4 CONTROLLA E UTILIZZA TUTTI I PUNTI DI CONNESSIONE

Porta la sicurezza oltre i confini tradizionali.

Sfrutta i tuoi router e switch per rilevare le minacce e garantirti l'enforcement con cui proteggere i tuoi ambienti di data center.

3 BLOCCAGGIO REALE DEGLI ATTACCHI

La verità: se la tua tecnologia di sicurezza non rileva le minacce conosciute, non vale il costo.

I dati non mentono! Fai una ricerca e scopri quali fornitori di sicurezza sanno rispondere davvero alle varie minacce e bloccano gli attacchi nella tua rete.

2 MANTIENI LE APPLICAZIONI ATTIVE

L'uptime deve essere garantito.

Il successo di un'azienda è legato al funzionamento della sua rete e alla connessione delle risorse. Il costo di una sicurezza efficace non può essere il downtime della rete. Verifica che le tue soluzioni di sicurezza siano affidabili, garantiscano un failover rapidissimo e il throughput necessario per la tua azienda.

1 CONTINUA A FARE PROGRESSI!

Non ti fermare.

Non preoccuparti se non tutto ti è chiaro. Il tuo interesse per Zero Trust è già un ottimo inizio. Inizia scegliendo un primo elemento da implementare e nel tempo avrai il tuo data center Zero Trust. Un passo alla volta è meglio che restare fermi.

Puoi farcela!

NON DIMENTICARE L'EDGE!

I dati sono il cuore di ogni iniziativa di sicurezza. Il segreto per mantenere protetto il data center è garantire una sicurezza efficace anche all'edge per proteggere l'accesso ai dati. Proteggi l'accesso di utenti e dispositivi alle applicazioni e ai dati che risiedono nei tuoi ambienti di data center e proteggerai in modo più efficace l'intera rete.

Juniper Networks

3050187-001-EN Ago 2023