CHECKLIST AKAMAI

Funzionalità della piattaforma Zero Trust

Un'efficace piattaforma Zero Trust combina singole soluzioni un tempo distinte, tra cui le funzionalità di microsegmentazione, ZTNA (Zero Trust Network Access), firewall DNS e ricerca delle minacce, in una piattaforma integrata con un'unica console. L'implementazione rapida ed efficace della piattaforma Zero Trust consente di bloccare i ransomware, soddisfare i rigorosi obblighi di conformità e proteggere la forza lavoro distribuita insieme all'infrastruttura cloud ibrida. Questa checklist risulta utile per valutare le funzionalità dei fornitori o come promemoria dei requisiti necessari per implementare il modello Zero Trust con una sola piattaforma.

Categoria 1. Requisiti della piattaforma

La piattaforma Zero Trust deve risultare flessibile, scalabile e facile da gestire.

- [ ] Scalabilità in grado di soddisfare le varie richieste di traffico e fornire una protezione continua senza peggiorare le performance
- [ ] Capacità di integrazione con gli strumenti di sicurezza esistenti, che i clienti utilizzano attualmente, ad esempio i sistemi SIEM, SOAR, EDR, CMDB e molti altri
- [ ] Copertura per data center eterogenei: ambienti ibridi e multicloud, sistemi legacy, dispositivi degli utenti finali, cluster Kubernetes, macchine virtuali, ambienti IoT/OT e altro ancora
- [ ] Modelli di distribuzione flessibili che supportano diverse architetture ibride: cloud, virtuali, on-premise
- [ ] Capacità di supportare distribuzioni basate su agenti e senza agenti (IoT/OT, PaaS)
- [ ] Supporto di Windows, Linux e macOS, nonché sistemi operativi tradizionali
- [ ] Funzionalità dei registri di controllo per garantire la registrazione di tutte le azioni

Categoria 2. Requisiti della visibilità

Una visibilità approfondita è fondamentale per comprendere l'ambiente, identificare connessioni sospette e rispondere in modo rapido e preciso alle minacce.

- [ ] Visualizzazione simile a una mappa di tutte le applicazioni e dei flussi dei carichi di lavoro, nonché dell'accesso degli utenti alle applicazioni in qualsiasi ambiente (container, senza server, IaaS o PaaS), il tutto da un'unica console
- [ ] Flussi storici e in tempo reale per indagini e analisi forensi
- [ ] Interoperabilità con firewall e hardware di terze parti come dispositivi switch
- [ ] Capacità di raccogliere dati da varie fonti di terze parti come CMDB, EDR e API cloud per etichette e regole contestuali
- [ ] Assistenza per l'etichettatura, preferibilmente utilizzando l'intelligenza artificiale per garantire velocità e precisione

Categoria 3. Requisiti delle policy

Sia le policy est-ovest (microsegmentazione) che nord-sud (ZTNA) vengono applicate da un'unica posizione sulla base di attributi che possono essere utilizzati in una serie di situazioni, come difesa dai ransomware, protezione della forza lavoro remota, risposta agli attacchi zero-day e conformità.

- [ ] Policy definita dal software e distribuita in tutta l'azienda senza richiedere firewall fisici interni in grado di creare punti di strozzatura
- [ ] Regole create in base a vari attributi dei carichi di lavoro anziché solo IP e porte
- [ ] Applicazione di policy granulari incentrate sulle applicazioni in modo che i carichi di lavoro siano protetti fino al livello di porte, processi e, persino, servizi
- [ ] Un motore di raccomandazione delle policy con modelli predefiniti e personalizzati, preferibilmente utilizzando l'intelligenza artificiale, che accelera la creazione delle policy
- [ ] Policy applicate con o senza agente
- [ ] Controlli delle policy basati sulla mappatura completa dei flussi
- [ ] Policy preconfigurate per ridurre i rischi globali sulla base delle best practice del settore
- [ ] Policy per il cloud ibrido in ambienti virtualizzati, IaaS e PaaS
- [ ] Policy legate ai carichi di lavoro con la possibilità di seguirli durante i loro spostamenti, migrazioni o cambiamenti
- [ ] Policy di accesso per gli utenti che lavorano in ufficio e da remoto

Categoria 4. Requisiti dei componenti Zero Trust

Tra le varie funzioni integrate in una piattaforma Zero Trust unificata, la soluzione Zero Trust Network Access e la microsegmentazione si distinguono come i pilastri fondamentali. Queste tecnologie consentono alle organizzazioni di implementare i controlli Zero Trust senza incidere negativamente sulla forza lavoro e sulla continuità operativa.

- [ ] Motore di accesso unificato e policy di rete (controllo combinato est-ovest e nord-sud)
- [ ] Efficace applicazione di policy basate sulle identità con l'autenticazione multifattore (MFA) FIDO2
- [ ] Capacità di proteggere gli ambienti IT e gli utenti da un'ampia gamma di minacce monitorando e filtrando il traffico DNS
- [ ] Rilevamento delle minacce elusive e monitoraggio del livello di sicurezza in modo costante
- [ ] Condivisione del segnale tra gli strumenti della piattaforma per assicurarsi di bloccare un criminale anche se riesce a superare il meccanismo di accesso
- [ ] Adozione di sistemi di frode dinamica in grado di tracciare e mettere in quarantena i criminali
- [ ] Capacità di eseguire query su endpoint o server per verificare la presenza di vulnerabilità in modo da consentire una rapida mitigazione del rilevamento dei ransomware

Categoria 5. Requisiti dell'intelligenza artificiale integrata

L'intelligenza artificiale può snellire molti aspetti alla base di un'implementazione efficace del modello Zero Trust per accelerare e semplificare la creazione di policy, la conformità, la risposta agli incidenti e la valutazione delle vulnerabilità.

- [ ] Comunicazione con i registri di rete utilizzando il linguaggio naturale per contribuire a ridurre i tempi di risposta agli incidenti, le operazioni di definizione dell'ambito della conformità e altro ancora
- [ ] Semplificazione dell'intero processo delle policy con l'intelligenza artificiale che suggerisce etichette e policy in base ad esclusivi modelli di traffico
- [ ] Conversione del linguaggio naturale in sintassi per individuare rapidamente eventuali vulnerabilità presenti nella rete senza dover ricercare IoC o scrivere query personalizzate
- [ ] Meccanismi di ricerca delle minacce basati sull'intelligenza artificiale per metodi di rilevamento avanzati in grado di individuare eventuali anomalie e attività dannose che gli strumenti tradizionali non riescono a rilevare

Per ulteriori informazioni, visitate la pagina dedicata alla sicurezza Zero Trust di Akamai.