Browser aziendale e SSE: insieme è meglio



Un browser aziendale fornisce un ambiente sicuro per i dispositivi non gestiti e per i dispositivi personali usati in ambito lavorativo (BYOD) che accedono al web, alle applicazioni e alle risorse aziendali. Tuttavia, se utilizzato da solo il browser aziendale spesso non offre l'ispezione del traffico TLS né controlli di sicurezza dei dati e DLP (Data Loss Prevention). L'integrazione di un browser aziendale con il Security Service Edge (SSE) consente non solo l'ispezione del traffico TLS e la protezione dei dati con DLP, ma anche una serie di ulteriori controlli di sicurezza, difese contro le minacce, accesso adattivo e formazione in tempo reale per gli utenti che compiono azioni a rischio.

Browser aziendale e Security Service Edge (SSE): Un lavoro di squadra più efficace

Lavorando insieme in modo integrato, il browser aziendale e l'SSE proteggono contro la perdita e il furto di dati causati da dispositivi non gestiti, da lavoratori temporanei che accedono ai dati e alle applicazioni aziendali, o durante fusioni e acquisizioni. Oggi 8 organizzazioni su 10 supportano l'accesso ai dati aziendali da dispositivi BYOD, permettendo agli utenti di accedere alle risorse di lavoro e aumentare la produttività[1]. Complessivamente, più di due terzi delle organizzazioni osservano un aumento della produttività abilitando l'accesso da dispositivi non gestiti[1].

Il BYOD introduce certamente sfide di sicurezza come la protezione dei dati, la conformità, il rischio di fuga o furto

di informazioni e l’accesso non autorizzato a dati sensibili. Questi dispositivi non rientrano sotto il controllo aziendale per quanto riguarda le policy, gli aggiornamenti o le applicazioni installate e potrebbero essere infetti, smarriti, rubati o compromessi. Sebbene il valore aziendale derivante dall’aumento della produttività sia elevato, le sfide di sicurezza del BYOD sono reali e non possono essere ignorate.

Tuttavia, anche se il dispositivo non è sotto il controllo dell’IT, è possibile controllare il browser web utilizzato per accedere a siti, applicazioni, conferenze, streaming video e webinar. Ad esempio, Netskope One Enterprise Browser è basato su Chromium ed è stato rafforzato disabilitando funzionalità non necessarie: protegge dall’impersonificazione del browser, crittografa le risorse, applica un rigoroso controllo delle estensioni con un design self-service e non richiede alcuna amministrazione per l’installazione. Una volta installato, offre uno spazio di lavoro autonomo per i collaboratori e i dispositivi BYOD, con indirizzamento alle funzionalità SSE tramite autenticazione con servizio di identità integrato e home page configurabili con collegamenti alle applicazioni rilevanti per ciascun gruppo di utenti.

Il potere dell’integrazione

L’integrazione di un browser aziendale con una piattaforma SSE è essenziale per il provisioning, l’autenticazione, il controllo delle policy in tempo reale, la formazione degli utenti e la protezione dei dati sia all’endpoint sia durante l’accesso attraverso l’ispezione SSE. Questa integrazione accelera il time-to-value e l’efficienza operativa, estendendo facilmente le policy di controllo delle applicazioni SSE agli utenti BYOD e ai collaboratori.

Alcuni punti chiave dell’integrazione riguardano la protezione dei dati su dispositivi non gestiti, con limitazioni su funzioni di copia, incolla e stampa; la sicurezza dei dati

inline SSE e DLP per web, applicazioni e servizi cloud; l'applicazione di controlli di policy per istanze specifiche di un'applicazione (aziendale vs personale); controlli delle policy in tempo reale specifici per il traffico su browser aziendale instradato all'ispezione SSE; riconoscimento di profili multi-tenant per collaboratori che lavorano con più aziende; maggiore agilità per supportare rapidamente nuovi utenti, collaboratori o progetti di M&A.

Ad esempio, gli utenti con dispositivi non gestiti o BYOD con browser aziendale installato possono accedere all'istanza aziendale di Google Drive all'interno dello spazio di lavoro sicuro, con le funzioni di copia e stampa bloccate, beneficiando al contempo della protezione dei dati inline SSE e della protezione dalle minacce. Tuttavia, potranno accedere alla loro istanza personale di Google Drive, ma non potranno trasferire file tra le due istanze.

Perché questo esempio? Secondo le ricerche di Netskope Threat Labs, nei 30 giorni precedenti la fine del rapporto di lavoro, il furto di dati aumenta del 300% e Google Drive è l'applicazione principale utilizzata per questo tipo di esfiltrazione[2].

Conclusioni

Un browser aziendale è più di un'isola autonoma per proteggere l'accesso al browser. I browser aziendali sono parte di una più ampia strategia di piattaforma unificata per SSE e SASE per l'accesso di dispositivi non gestiti e BYOD alla risorsa aziendale più importante: i dati.

Articolo a cura di **Tom Clare**, *Senior Director of Product Marketing, Netskope*

Fonti:

1. JumpCloud Critical BYOD Statistics to Know in 2024 – https://jumpcloud.com/blog/byod-statistics

2. Netskope Threat Labs – https://www.netskope.com/netskope-threat-labs/cloud-threat-report

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/browser-aziendale-sse/