Cloud Access Security Broker

Proteggi i dati in modo semplice in qualsiasi app cloud, con accesso da qualsiasi dispositivo

Sfida

- Proteggere e controllare gli accessi dai BYOD alle app gestite
- Controllare l'upload e il download di dati sensibili in qualsiasi app SaaS gestita
- Bloccare i malware nascosti nei file di dati di business
- Rilevare e controllare lo shadow IT

Soluzione

- Sicurezza delle app cloud con integrazione di DLP e protezione dalle minacce avanzate
- Controlli su dati e accessi Zero Trust granulari basati su utente, dispositivo o posizione
- Piattaforma AWS iper-scalabile per massimizzare i tempi di disponibilità dei servizi e ridurre al minimo la latenza
- Applicazione della DLP sui dispositivi gestiti e non gestiti

Risultato

- Aumenti la produttività, consentendo l'utilizzo delle informazioni ovunque in trasparenza e sicurezza
- Riduci i rischi grazie al controllo dei dati sensibili nel cloud e il blocco del malware
- Tagli i costi, semplificando le operazioni di sicurezza grazie a un pannello unificato per la configurazione delle policy
- Faciliti la conformità grazie a processi dimostrabili per il controllo delle informazioni

Per la forza lavoro ibrida di oggi l'accesso a dati e app nel cloud è oramai di routine. L'impresa media utilizza più di 280 app SaaS, tra cui strumenti di collaborazione come Microsoft 365, Google Workplace, Slack o Jira, diventati indispensabili per appaltatori e dipendenti che lavorano da remoto. L'uso di questi dispositivi senza una strategia per gestire gli accessi dai dispositivi mobili o stabilire se sono o meno affidabili (livello di sicurezza dei dispositivi) aumenta la complessità e i rischi.

Proteggere gli accessi alle app di business dai dispositivi BYOD e non gestiti
Forcepoint semplifica la sicurezza nel cloud. Il servizio di sicurezza CASB di Forcepoint ONE implementa l'accesso Zero Trust, che consente l'uso sicuro delle app cloud critiche dai dispositivi personali dei dipendenti (BYOD) e dai dispositivi non gestiti di partner e appaltatori.

Controllare l'upload e il download di dati sensibili in qualsiasi app SaaS gestita
Ti offriamo un insieme unificato di policy di sicurezza per controllare i dati sensibili con prestazioni al top del settore, a prescindere da dove e come dipendenti e appaltatori si connettono a internet. La gestione dell'accesso a queste app dai dispositivi mobili ne facilita l'adozione e favorisce la produttività, mentre la disponibilità di diverse policy basate sul livello di sicurezza e la posizione dei dispositivi offre un controllo Zero Trust granulare che mantiene i dati al sicuro. Avrai maggiore controllo sulle modalità con cui vengono condivisi i dati riservati nelle app aziendali su qualsiasi dispositivo, anche quelli personali. La DLP (Data Loss Prevention) è integrata, perciò non ti occorrono prodotti mirati per bloccare le violazioni dei dati.

Bloccare i malware nascosti nei file di dati di business
Il nostro CASB è in grado di rilevare e bloccare i malware nei dati in transito tra gli utenti e l'app SaaS, con motori per malware di Bitdefender e CrowdStrike. Può rilevare i malware anche nei file presenti nei più diffusi spazi di archiviazione SaaS e IaaS e metterli in quarantena.

Rilevare e controllare lo shadow IT
Oltre a portare allo scoperto lo shadow IT, il CASB offre anche controllo e coaching sull'uso sicuro e le alternative migliori. Il CASB rileva ed elenca le app SaaS non gestite in uso, consentendo agli amministratori di sviluppare policy per i dispositivi aziendali capaci di bloccare l'accesso o visualizzare un messaggio all'utente per indirizzarlo ad app SaaS autorizzate.

La soluzione CASB di Forcepoint ONE ottimizza uptime, disponibilità e produttività
Il nostro CASB fa parte di Forcepoint ONE, la nostra piattaforma cloud iperscalabile con 300 punti di presenza (PoP), accessibilità globale e un tempo comprovato di disponibilità dei servizi del 99,99%, per proteggere le app cloud in trasparenza e preservare la produttività degli utenti. Altre soluzioni deviano il traffico di rete alle/dalle applicazioni cloud verso date center privati piuttosto che verso postazioni vicine agli utenti. Ciò causa un degrado delle prestazioni, le app più soggette a problemi di latenza, come Slack, smettono di rispondere e i dipendenti finiscono per cercare rischiose soluzioni alternative.

Sicurezza cloud totale per ogni interazione

Semplificare la sicurezza del cloud nel mondo reale

La piattaforma cloud Forcepoint ONE offre un modo intuitivo per implementare la sicurezza nel cloud.

Da una sola console, gli amministratori possono gestire gli accessi e controllare i file scaricati e caricati dagli utenti sia sui dispositivi gestiti che su quelli non gestiti (ad esempio BYOD e computer di partner o di appaltatori).

Vediamo in che modo CASB semplifica la sicurezza cloud per Kris, analista commerciale che lavora da casa, quando comincia la sua giornata.

Kris accede al suo account Salesforce usando il laptop aziendale.	Il CASB in Forcepoint ONE gestisce le connessioni alle app di business, permettendo agli utenti di accedere in trasparenza e sicurezza.
Kris passa a salesforce.com direttamente o tramite un portale applicativo aziendale.	Salesforce ridirige la sessione sul CASB (tramite SAML), che analizza se il dispositivo è gestito, dove si trova e il suo livello di sicurezza. In base a policy di sicurezza predefinite, il CASB conferma l'identità di Kris tramite app di autenticazione a più fattori.
Kris è autorizzato ad accedere alle app gestite.	Le policy di amministrazione concedono l'accesso diretto all'app, l'accesso controllato oppure vietano del tutto l'accesso. Tutto questo accade nel giro di millisecondi, senza rallentare la produttività del dipendente. Tutto il traffico dall'app e dal dispositivo di Kris passa attraverso il CASB (usando un reverse proxy).
Kris decide di scaricare una previsione sulle entrate da Salesforce.	Il CASB analizza qualsiasi file scaricato dall'app per rilevare eventuali malware e dati sensibili. In base al risultato dell'analisi e alla policy, può bloccare i file contenenti malware, nonché bloccare, tracciare o crittografare i dati sensibili. Se una policy consente il download di dati sensibili solo su dispositivi gestiti, il download è consentito perché Kris sta usando un laptop aziendale.
Kris tenta di trasferire dati sensibili oppure un file contaminato da malware usando Slack, oppure cerca di caricare i dati nel suo spazio di archiviazione Dropbox personale.	Il CASB può controllare anche file che vengono caricati in app cloud. Il CASB può bloccare automaticamente l'upload. Può impedire persino l'upload dei file in app non autorizzate, usando l'agente unificato su dispositivo.

Parte di una soluzione di sicurezza unificata per app private, cloud e web

Oltre a CASB, la piattaforma all-in-one Forcepoint ONE protegge l'accesso alle informazioni di business su qualsiasi sito web e app privata:

- → **Web:** SWG monitora e controlla le interazioni con qualsiasi sito web in base a rischio e categoria, bloccando il download di malware o l'upload di dati sensibili in account e-mail e condivisioni di file personali. Il nostro SWG su dispositivo applica le policy d'uso accettabili sui dispositivi gestiti, ovunque siano.
- → **App private:** ZTNA protegge e semplifica l'accesso alle applicazioni private, senza le complicazioni o i rischi associati alle VPN.
- → **Altre funzionalità**, ad esempio RBI o l'analisi dei cloud provider per rilevare eventuali configurazioni rischiose (CSPM), in base alle necessità.

Per maggiori dettagli, leggi la Sintesi della soluzione Forcepoint ONE.

Vuoi proteggere i dati nelle app cloud da qualsiasi dispositivo?

Cominciamo con una demo.