Forcepoint

Sintesi della soluzione

Cloud Access Security Broker

Proteggi i dati 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

Nei nuovi modelli di lavoro odierni, gli utenti devono avere un accesso ai dati aziendali ovunque in modo rapido ma controllato. Pertanto, le persone hanno bisogno di accedere ai dati in applicazioni cloud come Microsoft 365, Google Workspace, Slack, Jira e Salesforce da qualsiasi tipo di dispositivo o posizione. Con oltre 250 app SaaS, è facile che la visibilità e il controllo per un'azienda media possa diventare ingestibile.

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 collaboratori esterni si connettono a internet. Gestire l'accesso a queste app dai dispositivi portatili facilita l'adozione e la produttività, mentre avere delle politiche diverse a seconda dell'identità e della posizione offre controlli Zero Trust granulari. La scansione inline per la ricerca di dati sensibili e malware protegge le informazioni in tutte le app SaaS. Saprai con maggiore certezza come i dati riservati vengono condivisi nelle app aziendali e, grazie alla funzione Data Loss Prevention (DLP) integrata, non avrai bisogno di prodotti specifici per bloccare le violazioni dei dati.

Bloccare i malware nascosti nei file di dati di business

Forcepoint ONE 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, CASB offre anche controllo e coaching sull'uso sicuro e le alternative migliori. CASB rileva le app SaaS non gestite in uso mediante i log di rete o la telemetria di Forcepoint ONE Secure Web Gateway, per consentire l'applicazione di politiche di sicurezza coerenti alle app SaaS sanzionate e non sanzionate, in modo che i dati aziendali siano al sicuro ovunque vengano utilizzati.

La soluzione CASB di Forcepoint ONE ottimizza uptime, disponibilità e produttività

CASB fa parte di Forcepoint ONE, la nostra piattaforma cloud iperscalabile con oltre 300 punti di presenza (PoP), accessibilità globale e un tempo comprovato di disponibilità dei servizi del 99,99%, per proteggere le applicazioni cloud con facilità e preservare la produttività degli utenti. Altre soluzioni deviano il traffico di rete da e verso le applicazioni cloud a dei data center privati invece di luoghi più vicini agli utenti e alle applicazioni a cui accedono. Ciò causa un degrado delle prestazioni e di conseguenza le app più soggette a problemi di latenza, come Slack, smettono di rispondere e i dipendenti finiscono per cercare rischiose soluzioni alternative.

Dati sicuri ovunque, per chi lavora da qualsiasi luogo

Semplificare la sicurezza del cloud nel mondo reale

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

Da un'unica console, gli amministratori possono gestire gli accessi e controllare i dati degli utenti sia di dispositivi gestiti che non gestiti (come i computer BYOD e quelli di collaboratori esterni e partner).

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 su CASB (tramite SAML), che analizza se il dispositivo è gestito, dove si trova e il suo livello di sicurezza. In base a delle policy di sicurezza predefinite, CASB conferma l'identità di Kris tramite l'autenticazione a più fattori.
Kris è autorizzato ad accedere alle app gestite.	Inoltre, 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 CASB (usando un reverse proxy o un forward proxy).
Kris decide di scaricare una previsione sulle entrate da Salesforce.	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 limita il download di dati sensibili ai dispositivi non gestiti, il download è consentito perché Kris sta usando un laptop aziendale.
Kris tenta di trasferire dati sensibili o un file contaminato da una malware tramite Slack.	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.
- **Ulteriori funzionalità** come la scansione dei provider cloud per le configurazioni rischiose Cloud Security Posture Management (CSPM) e SaaS Security Posture Management (SSPM), se necessario.

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

Vuoi proteggere i dati nelle app cloud da qualsiasi dispositivo?

Cominciamo con una demo.

forcepoint.com/contact