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 SaaS con DLP integrato 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

I nuovi modelli di forza lavoro odierni richiedono che gli utenti abbiano accesso rapido ma controllato ai dati aziendali ovunque. Ciò significa che le persone hanno bisogno di accedere ai dati nelle app SaaS come Microsoft 365, Google Workspace, Slack, Jira e Salesforce da qualsiasi tipo di dispositivo o posizione. Con oltre 250 app SaaS per l'azienda media, la visibilità e il controllo possono facilmente diventare ingestibili.

Proteggere gli accessi alle app di business dai dispositivi BYOD e non gestiti

Forcepoint semplifica la sicurezza del cloud. Il servizio di sicurezza CASB di Forcepoint ONE implementa l'accesso Zero Trust che consente alle app SaaS business-critical di essere utilizzate in modo sicuro 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 può rilevare e bloccare i malware nei dati in movimento tra gli utenti e l'app SaaS utilizzando più motori anti-malware di terze parti. 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

Forcepoint ONE CASB mette in luce lo shadow IT e genera una classificazione del rischio per le app non autorizzate analizzando attributi multipli. Ciò consente ai team IT di comprendere meglio l'utilizzo del SaaS all'interno della propria organizzazione e di applicare i protocolli di sicurezza necessari. CASB rileva le app SaaS non gestite in uso utilizzando i log di rete dei firewall e dei proxy aziendali per consentire l'applicazione di policy di sicurezza coerenti alle app SaaS sanzionate e non sanzionate, in modo che i dati aziendali rimangano al sicuro ovunque vengano utilizzati.

Soluzione per la sicurezza SaaS che massimizza i tempi di attività, la disponibilità e la produttività

Il nostro CASB è basato su un'architettura cloud-native basata sull'iperscalabilità con oltre 300 punti di presenza (PoP), accessibilità globale e un tempo di attività comprovato del 99,99% per proteggere le applicazioni SaaS in modo trasparente e preservare la produttività degli utenti. Altre soluzioni deviano il traffico di rete da e verso le applicazioni SaaS verso data center privati anziché verso posizioni più vicine 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

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 anche controllare i file caricati nelle app SaaS. Il CASB può bloccare automaticamente il caricamento. Può impedire persino l'upload dei file in app non autorizzate, usando l'agente unificato su dispositivo.

Parte dell'approccio alla protezione dei dati ovunque di Forcepoint

La missione di protezione dei dati ovunque di Forcepoint consente alle organizzazioni di proteggere i dati su SaaS, web, e-mail, rete ed endpoint, in modo che le persone possano lavorare in modo sicuro ovunque e con i dati ovunque.

Estensione delle funzionalità DLP leader del settore alle applicazioni SaaS

Con Forcepoint, le organizzazioni possono utilizzare le loro policy Forcepoint DLP esistenti per proteggere i dati nelle applicazioni SaaS, estendendo la stessa protezione dei dati leader del settore al cloud con pochi semplici clic. Le policy DLP unificate applicate da un'unica console aiutano a fornire una protezione dei dati consistente di classe enterprise per le applicazioni SaaS, semplificando la gestione della protezione dei dati, riducendo al minimo le violazioni e semplificando al contempo la conformità. I clienti possono trarre i seguenti vantaggi attraverso questa integrazione:

- → Protezione dei dati nel cloud semplificata con policy e console unificate.
- → 1.700 classificatori e modelli di policy pronti all'uso per una copertura completa e il supporto della conformità per oltre 150 regioni.
- → Configurazione della configurazione e time-to-value in pochi minuti, migliorando la produttività dei team IT/sicurezza.
- → Eliminazione dei prodotti per la sicurezza ridondanti e frammentati per ottenere risparmi significativi.

Leggi la brochure Forcepoint DLP per maggiori dettagli.

Vuoi proteggere i dati nelle app cloud da qualsiasi dispositivo?

Cominciamo con una demo.

forcepoint.com/contact