Forcepoint

Sintesi della soluzione

Secure Web Gateway

Blocca le perdite di dati e gli attacchi malware, non la produttività

Casi d'uso

- Concedi ai tuoi dipendenti l'accesso sicuro e veloce al web
- Applica una policy d'uso accettabile
- Blocca l'upload di dati sensibili su siti web non autorizzati
- Impedisci l'ingresso dei malware sui dispositivi degli utenti senza ostacolare la fruibilità
- Rileva e controlla lo shadow IT
- Previeni l'esposizione dell'azienda ai dati privati degli utenti

Soluzione

- Sicurezza web veloce con integrazione di DLP e protezione dalle minacce avanzate
- Controlli dei dati e accesso granulare Zero Trust in base a gruppo di utenti, tipo di dispositivo, posizione dell'utente, categoria del sito web, punteggio di rischio del sito web e altri fattori
- L'architettura distribuita elimina i colli di bottiglia sulla piattaforma AWS, iper-scalabile e con un elevato tempo di disponibilità dei servizi
- Remote Browser Isolation (RBI) opzionale per navigazione e download sicuri

Risultati

- Aumenta la produttività, permettendo a tutti di navigare nel web ovunque siano, in trasparenza e sicurezza
- Riduce i rischi, tramite il controllo dei dati sensibili nel cloud e il blocco dei malware
- Taglia i costi, semplificando le operazioni di sicurezza visto che le policy sono configurate da un unico pannello

Il web offre vantaggi ma anche rischi Molte persone dipendono dal web per trovare informazioni necessarie per il loro lavoro, ma il web è anche fonte di pericoli: esfiltrazione dei dati, violazione delle policy HR, perdite di produttività e infezioni da malware. Visto che le conseguenze di eventuali falle della sicurezza di dati e persone si fanno di giorno in giorno più gravi, proteggere le interazioni sul web è un'esigenza strategica per le organizzazioni moderne.

Concedi ai tuoi dipendenti l'accesso sicuro e veloce al web

La maggior parte degli SWG reindirizza forzosamente il traffico web in un data center centralizzato, in locale o nel cloud, aggiungendo così una latenza che può interferire pesantemente con le applicazioni web moderne. Viceversa, l'SWG in Forcepoint ONE ha un'architettura distribuita che elimina questi colli di bottiglia ed è in grado di raddoppiare il throughput per app e contenuti web dove le prestazioni hanno un'importanza critica. Tutto questo è possibile grazie a policy di sicurezza applicate localmente sul dispositivo dell'utente, per consentire il traffico diretto tra utente e sito web.

Applica controlli di policy sull'uso accettabile (AUP) sui siti web a rischio

Il web può essere fonte di innumerevoli distrazioni e non sempre viene utilizzato per scopo di lavoro. L'SWG di Forcepoint ONE permette di bloccare o autorizzare l'accesso a siti web non produttivi o non appropriati con un controllo completo dei percorsi; ad esempio, su Reddit, è possibile bloccare alcuni subreddit e consentirne altri. Gli accessi sono gestibili anche in base al gruppo di utenti, al livello di sicurezza del dispositivo, alla posizione, alla categoria dell'URL (predefinita o personalizzata), al punteggio della reputazione e alla classificazione aziendale del rischio dell'app. Le categorie di URL personalizzate possono includere percorsi di directory URL completi, per consentire agli amministratori di applicare policy diverse per diverse directory.

Blocca l'upload di dati sensibili su siti web non autorizzati

Con il nostro SWG puoi prevenire l'invio di proprietà intellettuale o dati regolamentati a supporti di archiviazione file personali, social media o account e-mail personali. Puoi scansionare e bloccare gli upload di file e i metodi Post HTTPS per i dati sensibili con gli stessi pattern DLP predefiniti e personalizzati utilizzati dai servizi CASB e ZTNA in Forcepoint ONE.

Impedisci l'ingresso dei malware sui dispositivi degli utenti senza ostacolare la fruibilità

Il nostro SWG offre svariate forme di protezione dai malware diffusi via web, inclusi i blocchi di categorie di siti web, la scansione in linea dei file scaricati e la protezione dalle minacce avanzate in base al principio Zero Trust, come la tecnologia Remote Browser Isolation. Con la nostra RBI, anche siti o file scaricati contaminati possono essere usati in sicurezza e con efficienza.

Rileva e controlla lo shadow IT

Il servizio SWG funziona insieme al nostro CASB per identificare i siti web utilizzati al posto delle app aziendali preferite. Questi siti "shadow IT" vengono acquisiti e visualizzati automaticamente nella console.

Previeni l'esposizione dell'azienda ai dati privati degli utenti

Per proteggere la privacy dei dipendenti, le organizzazioni possono prevenire la decrittografia e l'ispezione del traffico tra specifiche categorie di siti web solitamente utilizzate con informazioni di identificazione personale (PII), ad esempio dati bancari, sanitari e assicurativi.

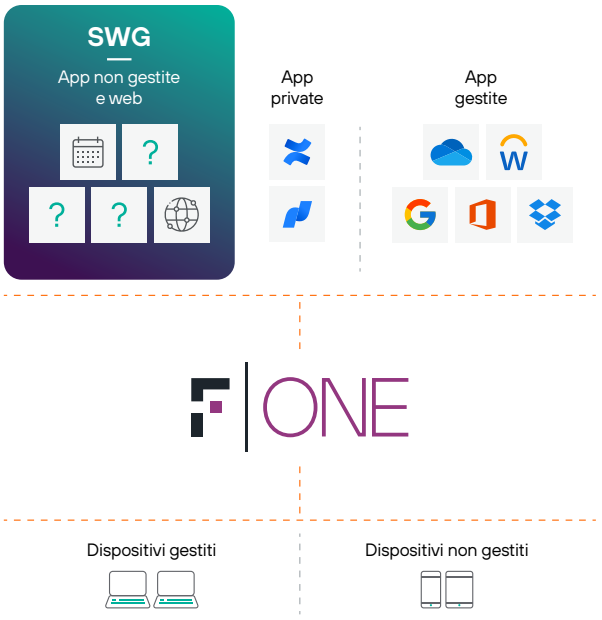
La soluzione SWG di Forcepoint ONE ottimizza uptime, produttività e prestazioni

SWG 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 gli accessi web e preservare la produttività degli utenti. Forcepoint ONE unifica CASB, SWG e ZTNA per proteggere gli accessi alle app private, web e SaaS aziendali, semplificando la sicurezza.

Semplificare la sicurezza web nel mondo reale

La piattaforma cloud Forcepoint ONE offre un pulsante rapido per attivare la sicurezza nel cloud.

Da una sola console, gli amministratori possono gestire gli accessi e controllare i download e upload di file tra un dispositivo gestito e qualsiasi sito web.



Dati sicuri ovunque, per chi lavora da qualsiasi luogo

Vediamo in che modo l'SWG semplifica la sicurezza web per Kris, analista commerciale che lavora da casa, quando comincia la sua giornata.

Kris naviga su reddit.com per fare ricerche per l'azienda.	Kris visita reddit.com/r/technology per ricercare gli ultimi post sui malware. Le policy sui contenuti SWG consentono una granularità a livello di directory: poiché questo subreddit è considerato correlato al lavoro, Kris può accedervi.
Nel subreddit r/technology Kris clicca accidentalmente un link verso un pagina inappropriata.	L'amministratore di Forcepoint ONE di Kris ha creato delle policy SWG per i contenuti che consentono l'accesso a directory come r/technology, ma lo impediscono a pagine e subreddit inappropriati. L'SWG blocca la svista di Kris impedendo l'apertura della nuova pagina.
Sul laptop aziendale, Kris comincia a compilare un foglio di calcolo riservato che include le PII di clienti e poi pensa di proseguire il lavoro sul suo laptop personale. Prova a caricare il file nel suo spazio di archiviazione cloud personale per scaricarlo sul suo laptop.	Per prevenire la perdita di dati aziendali, l'amministratore di Forcepoint ONE della società ha creato una policy SWG per i contenuti che blocca l'upload di informazioni sensibili dei clienti (PII) su qualsiasi sito web di condivisione di file personali. Quando Kris tenta di caricare il file, l'upload viene bloccato e appare un messaggio che spiega il motivo del blocco.

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

Oltre a SWG, la piattaforma all-in-one Forcepoint ONE protegge gli accessi alle informazioni di business su qualsiasi app privata e tenant SaaS aziendale:

- **Cloud (SaaS e IaaS):** CASB applica il controllo degli accessi in base al contesto, la DLP (Data Loss Prevention) e la protezione anti-malware a qualsiasi app web pubblica che supporta l'integrazione SAML 2 con fornitori di identità di terze parti (IdP), da qualsiasi browser moderno e su qualsiasi dispositivo connesso a internet. Anche i dati a riposo nei servizi IaaS e SaaS più diffusi possono essere analizzati per rilevare la presenza di dati sensibili e malware e adottare opportune contromisure di remediation. Per le app web private sono utilizzati gli stessi pattern di corrispondenza DLP disponibili per SWG e ZTNA.
- **App private:** ZTNA protegge e semplifica l'accesso alle applicazioni private, senza le complicazioni o i rischi associati alle VPN. Come altre soluzioni Forcepoint ONE, anche ZTNA applica il controllo degli accessi in base al contesto, DLP e protezione anti-malware a qualsiasi app web privata.
- **Funzionalità aggiuntive:** come RBI per la migliore protezione dalle minacce web, o Cloud Security Posture Management (CSPM) per analizzare i provider cloud per le configurazioni rischiose.
- **Cloud Firewall:** un componente SWG aggiuntivo per proteggere tutto il traffico internet e metterlo al sicuro dagli attacchi progettati per sfruttare le filiali vulnerabili.

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