

Forcepoint ONE Web Security

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
- › Previene 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 sulle piattaforme con uptime elevato
- › Include l'isolamento del browser in remoto (RBI) per la navigazione sicura e i download da siti non categorizzati e di nuova registrazione

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
- › Riduzione dei costi grazie alla semplificazione delle operazioni di sicurezza

Il web è sia una benedizione che una maledizione. La maggior parte delle persone dipende da esso per la ricerca di informazioni per svolgere il proprio lavoro, tuttavia, il web porta con sé rischi di esfiltrazione dei dati, violazioni delle policy HR, perdita di produttività e infezione da malware. La GenAI ha solo aumentato la posta in gioco: da un lato promette di aumentare enormemente la produttività, dall'altro espone le organizzazioni a molti più rischi. Tuttavia, con l'implementazione di misure di sicurezza adeguate, puoi sfruttare tale miglioramento della produttività che l'IA può offrire, mantenendo al contempo i dati sensibili al sicuro e assicurandone un utilizzo accettabile. Le conseguenze della mancata protezione dei dati e delle persone sono costantemente in aumento e la sicurezza delle interazioni web è un requisito strategico chiave per le organizzazioni moderne.

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

La maggior parte delle moderne soluzioni di sicurezza web costringe tutto il traffico web a deviare attraverso un centro dati centralizzato, sia in locale che nel cloud, aggiungendo una latenza che può interferire notevolmente con le moderne applicazioni web. Inoltre, nonostante le architetture cloud siano progettate appositamente per la scalabilità su richiesta, molti fornitori di SWG non hanno una presenza cloud così altamente distribuita. Al contrario, Forcepoint ONE presenta un'architettura distribuita che non solo fornisce una struttura cloud altamente resiliente, con oltre 300 punti di presenza in tutto il mondo, ma va oltre grazie a un'opzione alternativa in grado di offrire ai clienti ancora più flessibilità, l'agente on-device che elimina i colli di bottiglia e può consentire fino al doppio della velocità effettiva per i contenuti web sensibili alle prestazioni e le app come i gateway web sicuri concorrenti. Questa opzione applica le policy di sicurezza a livello locale sul dispositivo dell'utente in modo che il traffico possa essere scambiato direttamente tra l'utente e il sito web.

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

Il web può essere una fonte di distrazione e non sempre viene utilizzato per le attività aziendali. I controlli web di Forcepoint ONE consentono di bloccare, utilizzare una pagina di conferma, introdurre un tempo di utilizzo massimo, richiedere l'autenticazione a più fattori, consentire o persino utilizzare la RBI per isolare il traffico. La gestione degli accessi può essere eseguita in base al gruppo di utenti, alla postura del dispositivo e alla posizione. Ciò consente alle organizzazioni di mettere in atto controlli per bloccare l'uso dello shadow IT dei siti GenAI, ad esempio per la generazione di codice tramite una pagina di blocco per la ridirezione alle risorse con sanzioni aziendali, oltre a consentire una granularità tale da distinguere tra altri tipi di siti di IA, ad esempio per consentire di accedere ai siti IA di tipo conversazionale o multimediale, applicando al contempo misure di protezione dei dati che possono essere pubblicati su tali siti.

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

Grazie al nostro engine di sicurezza, è possibile impedire l'invio di dati regolamentati o protetti da proprietà intellettuale su file di archiviazione personali, social media, account di posta elettronica o siti GenAI. Consente di scansionare e bloccare il caricamento di file e i messaggi di testo con dati sensibili grazie a controlli facili da usare. Opzionalmente, i clienti possono ereditare le policy DLP avanzate di Forcepoint ONE Data Security per potenziare ulteriormente la soluzione di sicurezza avanzata dei dati leader nel settore.

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

Il servizio Forcepoint ONE Web Security offre molteplici misure di protezione contro i malware web-borne, includendo il blocco di categorie di siti web, la scansione in linea dei file scaricati e funzionalità di protezione avanzata dalle minacce zero-trust come l'isolamento remoto del browser. Con Forcepoint RBI, anche i siti o i file scaricati che sono stati contaminati possono essere utilizzati in modo sicuro ed efficiente.

Rileva e controlla lo shadow IT

Il servizio di sicurezza web individua i siti web che vengono utilizzati al posto delle app aziendali preferite. Questi siti "ombra" vengono raccolti automaticamente e visualizzati nella dashboard delle app cloud.

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

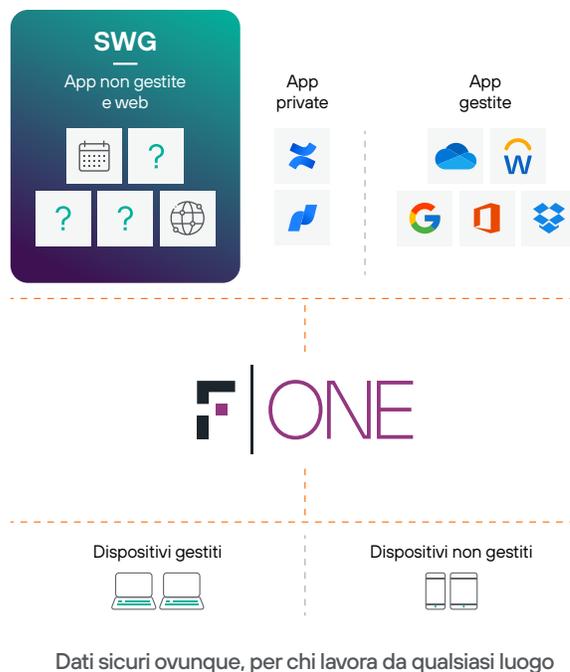
Per proteggere la privacy dei dipendenti, le organizzazioni possono prevenire la decrittografia e l'ispezione del traffico tra specifiche categorie di siti web solitamente utilizzate con informazioni di identificazione personale (PII), ad esempio dati bancari, sanitari e assicurativi.

Forcepoint ONE Web Security massimizza i tempi di uptime, la produttività e le prestazioni

Il servizio di sicurezza Web fa parte di Forcepoint ONE, la nostra piattaforma cloud avanzata con 300 punti di presenza (PoP), accessibilità globale e un uptime comprovato del 99,999% per proteggere gli accessi web e preservare la produttività degli utenti. Forcepoint ONE integra le tecnologie CASB, SWG e ZTNA per rendere sicuro l'accesso alle app aziendali SaaS, web e private, semplificando la sicurezza.

Semplificare la sicurezza web nel mondo reale

Da una singola console, gli amministratori possono gestire gli accessi e controllare i download e i caricamenti in tempo reale per qualsiasi sito e possono inoltre applicare le policy di accesso web zero-trust utilizzando Forcepoint RBI.





Ecco come il servizio di sicurezza web semplifica la vita al business analyst Kris, quando inizia a lavorare da casa ogni mattina.

<p>Kris naviga su reddit.com per fare ricerche per l'azienda.</p>	<p>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.</p>
<p>Nel subreddit r/technology Kris clicca accidentalmente un link verso un pagina inappropriata.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>

Fa parte di una soluzione di sicurezza integrata per il web, il cloud e le app private

Oltre alla sicurezza web, la piattaforma di sicurezza cloud Forcepoint ONE mette al sicuro l'accesso alle informazioni aziendali su qualsiasi tenant SaaS aziendale e app privata:

- **Cloud (SaaS e IaaS):** la tecnologia CASB applica il controllo degli accessi contestuali, la prevenzione della perdita dei dati (DLP) e la protezione dai malware su qualsiasi app web pubblica che supporta l'integrazione con SAML 2 con i fornitori di identità di terze parti (IdP), da qualsiasi browser moderno e dispositivo connesso a Internet. I dati a riposo sulle piattaforme IaaS e SaaS più popolari possono anche essere scansionati per individuare eventuali dati sensibili e malware e risolti. Si integra con Forcepoint ONE Data Security per applicare policy DLP avanzate sui canali SSE.
- **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.
- **Capacità aggiuntive:** espande il livello essenziale della RBI con il CDR, per un utilizzo che va ben oltre i siti web sconosciuti o di registrazione recente, per una protezione avanzata dalle minacce web, è inoltre possibile aggiungere funzionalità di rilevamento e protezione avanzata dai malware per il sandboxing e l'analisi aziendale.

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