Forcepoint

Sintesi della soluzione

Forcepoint ONE: la piattaforma cloud che semplifica la sicurezza per la forza lavoro ibrida

Casi d'uso

- Ottieni visibilità e controllo sul modo in cui i dipendenti che lavorano in modalità ibrida interagiscono con i dati di app private, cloud e web.
- Previeni usi scorretti dei dati sensibili raggiunti da dispositivi gestiti o non gestiti.
- Controllo degli accessi per contenuti web ad alto rischio e diversi tipi di siti GenAI.
- Offri accesso veloce e sicuro da remoto alle risorse di business e alle app private, senza le complessità delle VPN.

Soluzione

- La piattaforma unica consente la gestione coerente delle policy di sicurezza in tutte le app aziendali.
- Servizio all-in-one erogato via cloud che protegge accessi e dati grazie alla combinazione di Secure Web Gateway (SWG), Cloud Access Broker (CASB) e Zero Trust Network Access (ZTNA).
- Integrazione tra sicurezza dei dati e protezione dalle minacce avanzate per tenere fuori gli hacker e dentro i dati sensibili.
- Ulteriori funzionalità, come RBI, CSPM per la rilevazione delle configurazioni a rischio nei tenant cloud pubblici, CDR per la rimozione delle minacce dai contenuti e altro ancora.
- Classificazione Forcepoint per il tagging dei dati.

Risultato

- Semplificazione - accorpa la sicurezza per web, cloud e app private in un'unica piattaforma (con supporto senza agente).
- Modernità. Combina i principi Zero Trust con un'architettura SASE e tecnologie di sicurezza avanzate, come Remote Browser Isolation e la sanificazione dei file scaricati.
- Disponibilità. È disponibile globalmente, con oltre 300 punti di presenza (PoP).
- Affidabilità. Assicura un tempo di disponibilità verificato del 99,99%, dal 2015.
- Velocità. Usa l'applicazione distribuita e il ridimensionamento automatico per eliminare i colli di bottiglia.

Sicurezza data-first

Il mondo della sicurezza sta diventando sempre più complesso, ma c'è una soluzione. Ora che gli utenti lavorano da qualsiasi luogo, i dati sono dovunque, dai siti web alle app cloud e private.

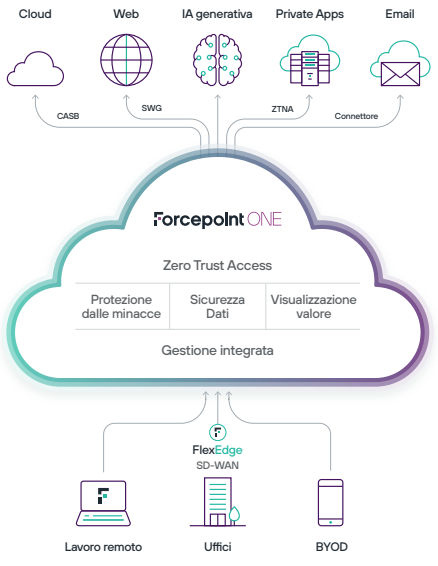
Per supportare al meglio il rientro in presenza e il lavoro ibrido, i team di sicurezza hanno bisogno di una piattaforma convergente che metta i dati al centro di tutto. I controlli di sicurezza devono poter essere estesi a tutti gli accessi al web, al cloud e alle app private, con una visibilità e un controllo coerenti, in modo che le organizzazioni possano darsi da fare per fermare le eventuali perdite di dati prima che si verifichino.

Con una soluzione data-first, i dati aziendali possono essere protetti ovunque, per una forza lavoro che opera dovunque.

Forcepoint ONE semplifica la sicurezza

Forcepoint ONE è la piattaforma cloud integrata che semplifica la sicurezza. Consente di adottare rapidamente un approccio zero trust e il Security Service Edge (SSE, la componente di sicurezza di SASE) perché abbiamo riunito servizi di sicurezza cruciali, tra cui SWG, CASB e ZTNA.

Migliora la produttività adottando in modo sicuro le nuove tecnologie come la GenAI, controllando gli accessi a diversi tipi di siti GenAI e applicando in modo coerente misure di protezione per tutelare i dati sensibili e prevenire l'esposizione ai malware.



Dati sicuri ovunque, per chi lavora da qualsiasi luogo

Le funzionalità Zero Trust di Forcepoint ONE, nate per il cloud, includono:

- **Sicurezza DLP senza agente per app cloud e private.** Utilizza in modo sicuro le app Web aziendali private dai dispositivi personali, mantenendo al sicuro i dati sensibili.
- **Protezione dalle minacce avanzate e sicurezza integrata dei dati.** Previeni la perdita o l'esfiltrazione dei dati e ferma gli hacker con controlli coerenti, ovunque.
- **Gateway unificati per l'accesso al cloud, al web e alle app private.** Controllo degli accessi alle app aziendali basato sull'identità e gestito in un unico posto per il SWG, il CASB e lo ZTNA.
- **Scalabilità dinamica con accesso globale.** 300 PoP realizzati su AWS offrono una connettività veloce e a bassa latenza, oltre a un uptime del 99,99%, a prescindere da dove si trova la tua forza lavoro..

Sicurezza unificata per app private, cloud e web

- **Cloud:** CASB applica l'accesso granulare a dati e app SaaS aziendali, da qualsiasi dispositivo. CASB blocca il download di dati sensibili e l'upload di malware in tempo reale. Analizza i dati a riposo nei SaaS e IaaS più diffusi per rilevare malware e dati sensibili e applica correzioni come necessario. CASB rileva le app shadow IT e controlla gli accessi da qualsiasi dispositivo gestito.
- **Web:** la piattaforma SWG monitora e controlla le interazioni con qualsiasi sito web, in base al rischio e alle categorie, bloccando il download di malware o l'upload di dati sensibili sui file di condivisione e sugli account di posta elettronica personali. La nostra sicurezza web on-device applica policy di utilizzo accettabili sui dispositivi gestiti, dovunque si trovino.
- **App private:** ZTNA protegge e semplifica gli accessi alle applicazioni private, senza le complicazioni o i rischi associati alle VPN.

Integrazione di protezione dalle minacce avanzate e sicurezza dei dati

- **Data Loss Prevention (DLP):** file e testi vengono analizzati in upload e download per individuare eventuali dati sensibili e bloccarli, tracciarli, crittografarli oo oscurarli, come appropriato.
- **Scansione anti-malware:** i file vengono analizzati in upload e download per individuare eventuali malware e bloccarli.

Visibilità e controllo integrati

- **Suite di gestione integrata** per la configurazione, il monitoraggio e la creazione di report su tutti i canali SSE.
- **Policy di login** per il controllo degli accessi alle applicazioni web, cloud o private in base alla posizione dell'utente, al tipo di dispositivo e alla sua posizione, al comportamento e al gruppo di utenti. Questi parametri aiutano a prevenire i possibili takeover degli account.
- **Policy DLP facili da usare,** per il controllo dei download e il caricamento di dati sensibili e malware per le app SaaS gestite, le app private e i siti web, nonché per i dati archiviati in SaaS e IaaS gestiti.
- **Agente on-device** per Windows e MacOS per il supporto di SWG, CASB o ZTNA per app client di tipo non-browser e il controllo dello shadowing IT.
- **Rappresentazione grafica dei valori e analisi unificate** per informazioni veloci e approfondite sui rischi per la sicurezza, l'utilizzo globale e l'impatto della piattaforma di sicurezza cloud all-in-one.

Funzionalità aggiuntive disponibili in base a necessità

- **Cloud Security Posture Management (CSPM):** esamina le impostazioni dei tenant GCP, Azure e AWS per individuare le configurazioni rischiose; offrendo possibilità di correzioni manuali e automatizzate.
- **SaaS Security Posture Management (SSPM):** esamina le impostazioni dei tenant Office 365, ServiceNow e Salesforce per individuare le configurazioni rischiose; offrendo possibilità di correzioni manuali e automatizzate.
- **Remote Browser Isolation (RBI):** protegge gli utenti dai malware trasmessi via web sui dispositivi locali mettendo a disposizione un browser eseguito in una VM ospitata su cloud.
- **Forcepoint Classification:** data classification tagging con suggerimenti basati sull'IA per tag più accurati.
- **AMDP:** analisi del comportamento dei file in un sandbox malware controllato per identificare i contenuti nascosti e dannosi.

Abbonamenti che aprono un mondo di semplicità

Sono disponibili abbonamenti annuali per utente:

- **Edizione All-in-one** per la sicurezza di app private, web e cloud.
- **L'edizione di sicurezza Web** include il gateway web e la soluzione CASB inline per app cloud illimitate e opzioni RBI essenziali per siti non categorizzati o di nuova registrazione per l'aggiunta successiva del supporto API per le app cloud e per le app private.
- **L'edizione ZTNA** protegge un numero illimitato di applicazioni private.
- **L'edizione CASB** protegge un numero illimitato di applicazioni cloud in linea e include API per 3 applicazioni con la possibilità di aggiungere pacchetti di app aggiuntivi o nodi di polling API dedicati.
- **Tutti gli abbonamenti** includono la gestione cloud centralizzata, policy per la prevenzione della perdita dei dati, accessi automatizzati tramite agente endpoint e funzionalità di reporting complete.

forcepoint.com/contact