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.
- Controlla gli accessi ai contenuti web ad alto rischio.
- Offri accesso veloce e sicuro da remoto alle risorse di business e alle app private, senza le complessità delle VPN.

Soluzione

- Una singola piattaforma unificata consente di gestire un set unico di policy su tutte le app, da una sola console e attraverso un solo agente endpoint.
- 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 (dettagli a pag. 2).

Risultato

- Semplicità. Unifica la sicurezza per le app private, cloud e web in un singolo set di policy, con una sola console e un solo agente (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.

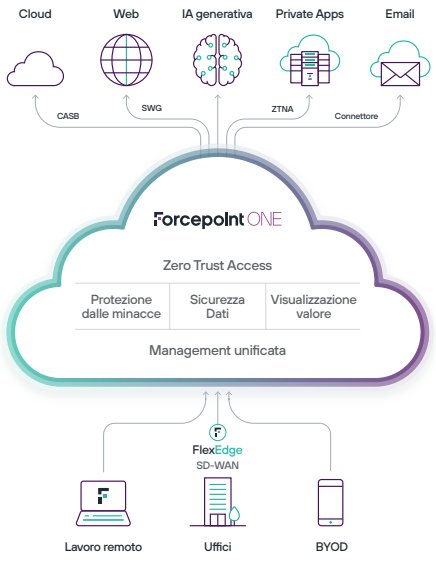
Per supportare al meglio il rientro in presenza e il lavoro ibrido, i team di sicurezza hanno bisogno di una piattaforma convergente che metta i dati al centro di tutto. I controlli di sicurezza devono poter essere estesi a tutti gli accessi al web, al cloud e alle app private, con una visibilità e un 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, le informazioni aziendali possono essere protette ovunque, così da consentire alle persone di lavorare dove desiderano.

Forcepoint ONE semplifica la sicurezza

Forcepoint ONE è una piattaforma cloud all-in-one che semplifica la sicurezza. Puoi adottare velocemente Zero Trust e Security Service Edge (SSE, il componente di sicurezza del SASE) perché abbiamo unificato i servizi di sicurezza essenziali, come Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) e Zero Trust Network Access (ZTNA).

Niente più prodotti frammentati. Ti diamo una sola piattaforma, una sola console e un solo agente, ma molte soluzioni. Ottieni visibilità, controlla gli accessi e proteggi i dati sulle app gestite e non gestite e su tutti i dispositivi, usando un solo set di policy di sicurezza.



Dati sicuri ovunque, per chi lavora da qualsiasi luogo

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

- **Sicurezza BYOD senza agente per app private e cloud.** Le app web di business private possono essere usate senza rischi dai dispositivi personali, mantenendo al sicuro i dati sensibili.
- **Integrazione tra sicurezza dei dati e protezione dalle minacce avanzate** su tutti i gateway, per prevenire esfiltrazioni o fughe di dati e impedire l'accesso agli hacker.
- **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:** 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 accettabile sui dispositivi gestiti, ovunque siano.
- **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.

Applicazione semplificata da un singolo set di policy

- **Una sola console di gestione** per la configurazione, il monitoraggio e i report.
- U**n solo set di policy di accesso** per il controllo degli accessi alle applicazioni web, cloud o private in base alla posizione dell'utente, al tipo di dispositivo, al livello di sicurezza del dispositivo, al comportamento dell'utente e al gruppo a cui appartiene. Questi parametri aiutano a prevenire violazioni di account.
- **Singolo set di policy DLP** per controllare il download e l'upload di dati sensibili e malware per app SaaS gestite, app private e siti web, nonché per i dati archiviati in IaaS e SaaS gestiti.
- **Agente unificato su dispositivo** per Windows e MacOS, per supportare SWG, CASB e ZTNA per il controllo di shadow IT e app client non su browser.
- **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.
- **Cloud Firewall:** componente SWG aggiuntivo per proteggere tutto il traffico internet e metterlo al sicuro dagli attacchi progettati per sfruttare le filiali vulnerabili.

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.
- **Edizione Web-security**, che permette ai clienti di aggiungere in un secondo momento il supporto per app private e cloud.
- **Tutti gli abbonamenti** includono gestione cloud centralizzata, policy unificate con DLP, accesso automatizzato mediante un agente endpoint unificato e report completi.

forcepoint.com/contact