Forcepoint ONE

Zero Trust Network Access

Semplifica la sicurezza per le app private, senza VPN

Casi d'uso

- Sostituzione delle VPN per l'accesso alle app private nei data center e nei cloud privati.
- Accesso sicuro e senza agente ad app web private da dispositivi BYOD e non gestiti.
- Controllo di upload e download di dati sensibili in qualsiasi app web privata.
- Blocco dei malware nascosti in file di dati di business provenienti da app web private o a queste destinati.
- Protezione dell'accesso ai server privati da dispositivi macOS e Windows gestiti.

Soluzione

- Sicurezza delle app private con integrazione di DLP e protezione dalle minacce avanzate.
- Controllo degli accessi Zero Trust senza agente per le app web private da dispositivi gestiti e BYOD.
- Accesso remoto alle app non web private da dispositivi macOS e Windows gestiti.
- Parte di una piattaforma cloud con SWG, CASB e altre funzionalità di sicurezza.

Risultato

- Aumenti la produttività, consentendo l'accesso alle app private ovunque in trasparenza e sicurezza.
- Tagli i costi, semplificando le operazioni di sicurezza grazie a un pannello unificato per la configurazione delle policy.
- Riduci i rischi grazie al controllo dei dati sensibili e del malware in transito alle/dalle app web private.
- Faciliti la conformità grazie a processi dimostrabili per il controllo delle informazioni.

Il lavoro da remoto ha messo in luce i limiti, i costi e i rischi delle reti private virtuali (VPN). Una volta che gli utenti sono connessi alla VPN, vengono considerati attendibili in modo implicito e hanno la possibilità di analizzare ed esaminare altri indirizzi IP dello stesso data center o cloud privato virtuale, diventando così potenziali vettori di violazioni. Le organizzazioni che vogliono passare dalle VPN a soluzioni ZTNA (Zero Trust Network Access) devono però poter evitare ulteriori complicazioni e l'aggiunta di prodotti mirati: l'adozione dell'accesso Zero Trust deve essere semplice e senza ostacoli.

La ZTNA di Forcepoint controlla l'accesso alle app private web e non web che ogni dipendente, appaltatore e partner è esplicitamente autorizzato a usare. Forcepoint ZTNA offre un controllo nettamente superiore e consente agli operatori di usare in sicurezza i dispositivi con cui si trovano meglio, anche non gestiti e BYOD.

Diversamente da altre soluzioni, Forcepoint ZTNA offre anche controlli costanti e granulari, prestazioni al top del settore e una protezione integrata dei dati e dai malware, per offrire una user experience eccellente nonostante le complessità delle reti moderne. In più, è facile aggiungere in base alle necessità altre soluzioni di sicurezza, come CASB (Cloud Access Security Broker) e SWG (Secure Web Gateway), tutte integrate perfettamente nella piattaforma cloud Forcepoint ONE.

RSostituzione delle VPN per l'accesso alle app private nei data center e nei cloud privati

Per proteggere l'accesso alle app private occorre un controllo veloce e mirato. Puoi limitare l'accesso alle app private come ERP o ai server della catena di fornitura in base all'identità, all'appartenenza a un gruppo e al tipo e alla posizione dei dispositivi. Nel caso delle app non web puoi applicare i controlli per porta e proteggere gli accessi da dispositivi o posizioni non noti. Se un tentativo di accesso appare sospetto, l'utente dovrà dimostrare la propria identità tramite l'autenticazione a più fattori (MFA). Con la piattaforma iperscalabile di Forcepoint, tutto questo accade in qualche millisecondo.

Accesso sicuro e senza agente alle app web private dai dispositivi BYOD

Gli utenti possono connettersi via internet in sicurezza e comodamente alle app web in hosting dietro un firewall, anche da dispositivi non gestiti e BYOD, senza bisogni di agenti.

Controllo di upload e download di dati sensibili in qualsiasi app web privata

Un solo set di policy di sicurezza consente di controllare i dati sensibili, con accesso a DLP e scansione anti-malware integrati per bloccare hacker e violazioni dei dati. La sicurezza dai dati combinata alle policy per la posizione e il livello di sicurezza dei dispositivi facilita il controllo del modo in cui gli utenti spostano i dati dalle/alle app web private su qualsiasi dispositivo.

Blocco dei malware nascosti in file di dati di business provenienti da app web private o a queste destinati

Forcepoint tiene sotto controllo il ransomware. Rileva e blocca il malware nei dati in transito tra utenti e qualsiasi app web privata con i motori di scansione Bitdefender e CrowdStrike.

Protezione dell'accesso ai server non web privati dai dispositivi gestiti

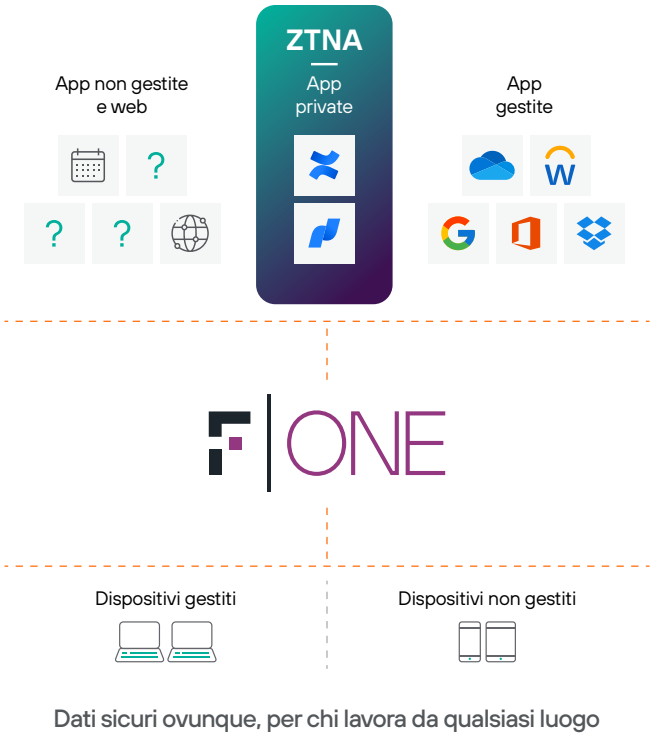
ZTNA protegge l'accesso da remoto per protocolli non web, come Secure Shell (SSH), e protocolli di desktop remoto (RDP) da Mac o PC gestiti con l'agente unificato Forcepoint ONE.

La soluzione ZTNA di Forcepoint ONE ottimizza uptime, disponibilità e produttività

ZTNA fa parte di Forcepoint ONE, la nostra piattaforma cloud iperscalabile con oltre 300 punti di presenza (PoP), accessibilità globale e un tempo comprovato di disponibilità dei servizi del 99,99%, per proteggere le app private con facilità e preservare la produttività degli utenti. Altre soluzioni deviano il traffico di rete attraverso data center privati piuttosto che verso postazioni vicine agli utenti, risultando così in prestazioni scarse. Forcepoint ONE unifica CASB, SWG e ZTNA per proteggere l'accesso alle app private, web e SaaS aziendali, semplificando la sicurezza.

Semplificare la sicurezza delle app private nel mondo reale

La piattaforma cloud Forcepoint ONE offre un modo intuitivo per implementare la sicurezza delle app private. Da una sola console, gli amministratori possono gestire gli accessi e controllare i file scaricati e caricati dagli utenti sia sui dispositivi gestiti che su quelli non gestiti (ad esempio BYOD e computer di partner o di appaltatori).



Dati sicuri ovunque, per chi lavora da qualsiasi luogo

Vediamo in che modo la funzionalità ZTNA semplifica la sicurezza delle app private per Kris, analista commerciale che lavora da casa, quando comincia la sua giornata.

Kris accede al suo account Forcepoint ONE usando il laptop aziendale.	Poiché sta usando un dispositivo gestito da una posizione autorizzata, Kris riesce a completare l'accesso. Un tentativo di accesso eseguito da una posizione sconosciuta richiede una risposta positiva attraverso un'app MFA.
Kris ottiene l'accesso con un clic all'applicazione della catena di fornitura di proprietà dell'azienda dal portale utenti di Forcepoint ONE.	Sul browser di Kris è visualizzato il portale di Forcepoint ONE, con riquadri per ogni app web accessibile a Kris e ai suoi partner della catena di fornitura (se la società di Kris usa Forcepoint ONE CASB, le app SaaS gestite di Kris sono accessibili dallo stesso portale utenti, per offrie un'esperienza coerente).
Kris è autorizzato ad accedere alle app gestite.	Il traffico tra il laptop di Kris e l'app della catena di fornitura passa automaticamente attraverso il reverse proxy di Forcepoint ONE. Forcepoint analizza i file in upload e download per rilevare eventuali malware e dati sensibili.
Kris carica il contratto di un fornitore come allegato.	Poiché la policy per la connessione di Kris specifica la scansione dei file, l'upload è consentito solo se il file non contiene malware. Se è infetto, il gateway ZTNA blocca l'upload, avvisa Kris e registra e segnala in un report l'evento di blocco.

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

Oltre a ZTNA, la piattaforma all-in-one Forcepoint ONE protegge l'accesso alle informazioni di business su qualsiasi sito web e app privata:

- **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 accettabili sui dispositivi gestiti, ovunque siano.
- **Cloud:** CASB protegge e semplifica l'accesso ai tenant IaaS e SaaS aziendali, controllando nel contempo la trasmissione di malware e dati sensibili, senza bisogno di un agente sul dispositivo.
- **Altre funzionalità,** ad esempio RBI o l'analisi dei cloud provider per rilevare eventuali configurazioni rischiose (CSPM), in base alle necessità.

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