Forcepoint

Ebook

Lavorare da remoto in sicurezza

Suggerimenti per la sicurezza dei team che lavorano fuori sede

Sommario

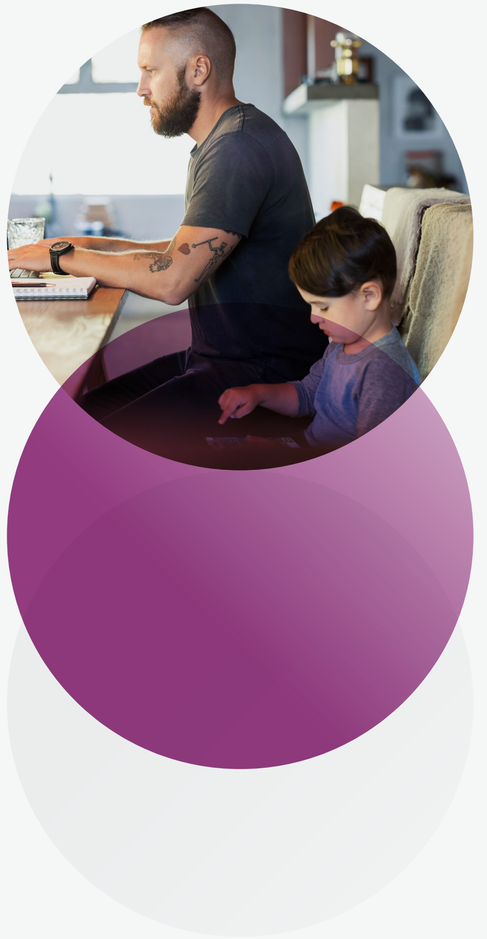
I rischi per la sicurezza da non sottovalutare quando si lavora da remoto

In un clima globale come quello odierno, è presumibile che sia sensibilmente aumentato il numero di dipendenti che lavorano da casa. Probabilmente hai già adottato delle strategie di sicurezza per far fronte a questo cambiamento improvviso, ma è difficile essere completamente preparati.

I rischi per la sicurezza da non sottovalutare quando si lavora da remoto

Quando i dipendenti lavorano da remoto, molte cose cambiano. Le ipotesi su come i dipendenti accedono alle applicazioni nel cloud o in locale e su come proteggerli, possono spesso ribaltarsi. Le soluzioni di Forcepoint possono contribuire alla sicurezza aziendale e alla produttività dei dipendenti, quando:

- Utilizzano l'e-mail aziendale, anche quando cliccando sui link
- Accedono a siti e contenuti web da reti Wi-Fi domestiche o pubbliche
- Accedono ai dati e li archiviano su applicazioni aziendali basate su cloud
- Si ricollegano alla rete aziendale per accedere ad app e dati interni



Probabilmente hai già adottato delle applicazioni basate sul cloud ed autorizzato alcuni dipendenti a lavorare mentre sono in viaggio o a casa. Ma i processi validi per un gruppo esiguo di persone possono risultare inadeguati se applicati su larga scala. Se hai già implementato dei prodotti Forcepoint per l'ufficio, alcune piccole modifiche ti permetteranno di usare i sistemi già in dotazione per proteggere i dipendenti che lavorano da casa o fuori sede.

La missione di Forcepoint è contribuire a promuovere ambienti sicuri e affidabili in modo da proteggere i dipendenti e i dati critici ovunque. Ecco alcuni suggerimenti veloci per consentire ai dipendenti di lavorare in modo efficiente e sicuro fuori ufficio.

Estensione della protezione antiphishing e-mail fuori dall'ufficio

Come molte aziende, probabilmente anche tu disponi già di un sistema di sicurezza e-mail configurato per fornire l'accesso remoto all'e-mail da dispositivi mobili o gestiti.

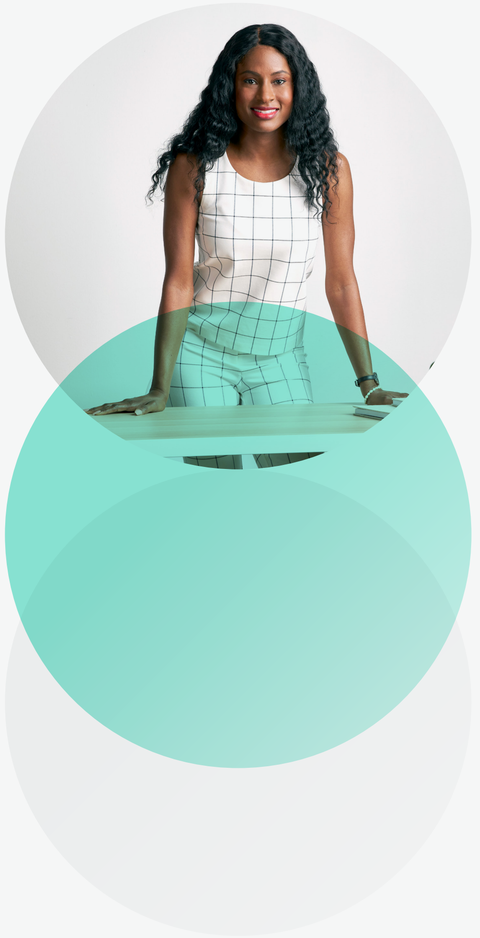
Estensione della protezione antiphishing e-mail fuori dall'ufficio

Con l'aumento del numero dei lavoratori a distanza, è una buona idea verificare che la posta elettronica sia protetta in entrambe le direzioni:

- → **In ingresso** – I messaggi e gli allegati inviati ai tuoi utenti devono essere ispezionati per verificare eventuali tentativi di phishing, ransomware, malware, spam e altri contenuti indesiderati.
- → **In uscita** – I messaggi e gli allegati inviati dai tuoi utenti devono essere analizzati per assicurare che dati sensibili, proprietà intellettuale e altre informazioni aziendali non vengano trasmessi senza autorizzazione (questa procedura spesso è indicata come Data Loss Prevention o DLP). Il traffico in uscita deve essere ispezionato anche per rilevare eventuali malware, in modo da evitare che i dipendenti possano infettare i tuoi clienti.

Se utilizzi Forcepoint Email Security e già consenti l'accesso da remoto alla posta elettronica, assicurati semplicemente che il Mail Transfer Agent collegato al sistema abbia, tra il sistema e internet, una capacità di rete sufficiente a supportare un incremento del traffico remoto.

I messaggi di phishing, che invitano gli utenti a cliccare su link apparentemente innocui, continuano ad essere la principale fonte di attacchi. La maggior parte dei sistemi di sicurezza e-mail segnala o blocca i link a siti web notoriamente dannosi, ma i siti web che nessuno ha ancora visitato potrebbero non essere bloccati. Gli operatori che lavorano fuori sede hanno bisogno di un sistema di sicurezza web che li protegga ovunque si trovino.



Protezione dei dipendenti che navigano nel web e lo utilizzano in modo diverso

In un panorama delle minacce in rapida evoluzione, se i tuoi impiegati hanno un metodo di lavoro diverso, queste differenze creano più rischi per la sicurezza. Devi, inoltre, tener conto del mix tra sfera lavorativa e vita privata, dell'impatto della protezione sulla vita quotidiana e di come tutelare la flessibilità.

Due considerazioni sono importanti:

- → Quanto sono protetti gli impiegati che lavorano fuori della rete aziendale? E quanto è protetta la tua organizzazione e i suoi dati?
- → Maggiore utilizzo del web, inclusa la navigazione a fini personali

Protezione dei dipendenti che navigano nel web e lo utilizzano in modo diverso

La tua azienda probabilmente è passata dal lavoro in sede al lavoro da casa. Le soluzioni tradizionali in locale, ad esempio un gateway web sicuro basato su dispositivo, purtroppo proteggono gli utenti solo quando sono in rete. Sebbene per qualcuno il passaggio al cloud sia stato fonte di preoccupazioni, in particolare nel contesto della rapida adozione delle soluzioni SaaS (di app cloud autorizzate e non autorizzate), in realtà il cloud è più un alleato che una minaccia, ora più che mai. Questo vale soprattutto per la Web Security. La rete aziendale deve fornire agli utenti a casa lo stesso livello di protezione che avrebbero in ufficio.

La Web Security basata su cloud consente ai dipendenti che lavorano da casa (che siano o meno nuovi all'esperienza) di accedere in modo sicuro ai contenuti web; si adegua al loro metodo di lavoro, senza limitarsi alle applicazioni cloud che utilizzano. In un momento in cui andare al lavoro è fuori discussione, mandare i figli a scuola è fuori discussione e prendere appuntamenti, partecipare a meeting e incontrarsi con gli altri – sia per lavoro sia per interessi personali – è fuori discussione, in che modo puoi affrontare il problema? L'incremento nell'uso del web è sicuro: i dipendenti, che ora lavorano da remoto, rimangono connessi leggendo le notizie, usando LinkedIn e il web per continuare con le loro attività quotidiane. Tra l'uso del web per motivi professionali e la navigazione a scopo personale, la protezione dell'azienda contro le minacce in circolazione sul web è cruciale.

La Web Security basata su cloud di Forcepoint assicura la protezione degli utenti, ovunque svolgano il loro lavoro. L'accesso al web sarà sempre necessario e il mantenimento della produttività e del giusto equilibrio tra accesso sicuro e protezione solida (ma flessibile) è fondamentale per proteggere persone e dati.

Garanzia di sicurezza dei dati in un ambiente multi-cloud

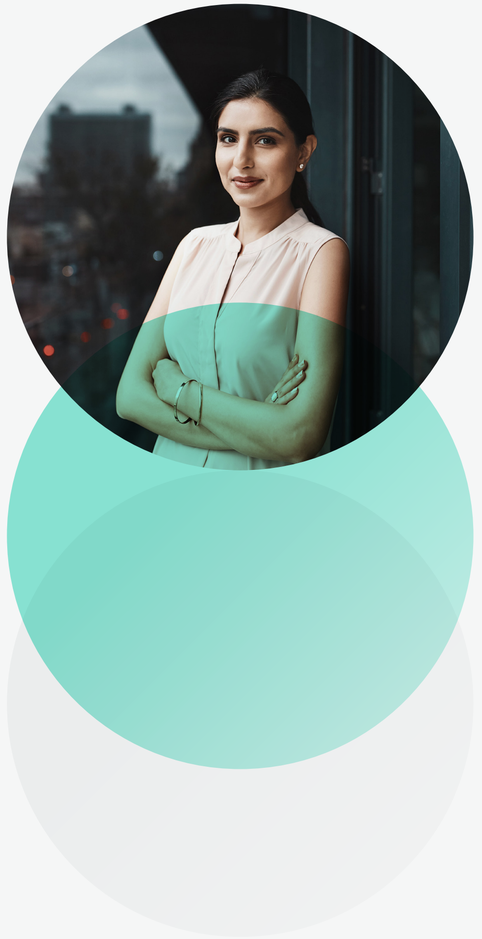
La sicurezza nel cloud è molto spesso una responsabilità condivisa: il fornitore di servizi cloud si occupa della sicurezza della propria infrastruttura, mentre la protezione di dati e attività degli utenti aziendali nell'ambito di quella stessa infrastruttura spetta alle aziende.

L'azienda, in sintesi, è responsabile di fattori come il comportamento degli utenti, gli accessi, le policy dei dati, le policy di utilizzo e la conformità legale. Questo vale sia per i dispositivi gestiti che per quelli non gestiti in un modello di lavoro da remoto.

Garanzia di sicurezza dei dati in un ambiente multi-cloud

Tutte le aziende si avvalgono di strumenti per la protezione dei dati critici e della proprietà intellettuale. Se tu hai adottato una soluzione DLP, il primo passo per ottimizzarla per il lavoro da remoto è l'analisi delle policy. Comincia dai dati critici di back-office che forse hai dovuto spostare velocemente nel cloud: hai la certezza che in questo momento l'accesso sia limitato ai soli utenti autorizzati? Sfrutta le policy predefinite per questo tipo di dati e ottimizzale. Nel caso delle informazioni altamente sensibili, puoi implementare il fingerprinting dei dati e adottare policy in grado di controllare questi dati ovunque vengano spostati, nonché implementare policy restrittive basate sullo spostamento.

Successivamente puoi valutare l'implementazione di policy per la perdita dei dati, che possono rilevare e impedire spostamenti impercettibili dei dati e garantire la sicurezza, soprattutto per i dati regolamentati o personali. Allo stesso tempo, assicurati che le policy consentano il reporting dei dati dall'endpoint al cloud, al fine di mantenere la conformità.



Garanzia di sicurezza dei dati in un ambiente multi-cloud

Molte aziende decideranno che è giunto il momento di sottoporre i dati a controlli più specifici per le applicazioni cloud che non sono state abilitate in modo tradizionale. È proprio qui che una soluzione come Forcepoint CASB può essere d'aiuto, fornendo visibilità e controllo su applicazioni cloud autorizzate e non autorizzate e su dispositivi gestiti e non gestiti. E, come sosterrebbe qualsiasi esperto in sicurezza, le difese perimetrali per la rete e la protezione degli endpoint non bastano.

Forcepoint mette in primo piano il comune denominatore di ogni scenario: l'utente. Forcepoint CASB offre approfondimenti sui modelli di utilizzo e sui profili dei dispositivi, implementa le policy in modo proattivo e protegge gli account sugli endpoint gestiti e non gestiti. Questa strategia è fondamentale per rilevare e contrastare ogni attività anomala in modo da proteggere utenti e dati nel cloud. A questo punto il sistema di protezione dati di Forcepoint facilita il consolidamento dell'assetto di sicurezza dei dati, unificando le policy dei dati su tutti i canali (endpoint, rete e cloud) a partire da un'unica console.

Come ultima mossa, valuta la possibilità di ampliare il quadro generale della protezione dei dati e dove è implementata all'interno dell'azienda. Che si tratti di allargare il controllo degli endpoint in remoto per includere un gruppo più ampio di utenti, di prevenire le violazioni dei dati con policy proattive e adattive al rischio o di ampliare la visibilità e il controllo sull'accesso alle applicazioni cloud o sullo spostamento dei dati, Forcepoint può aiutarti a creare un piano e/o fornire i servizi necessari per tenere al sicuro i dati, ovunque si trovino e ovunque siano i tuoi collaboratori.

Connessione dei lavoratori in remoto ad applicazioni e dati interni

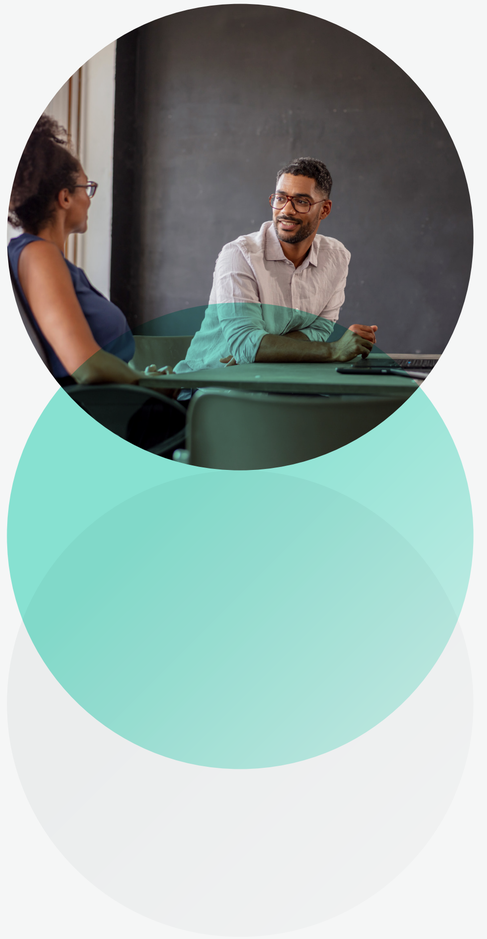
Nonostante gran parte delle applicazioni e dei dati necessari ai tuoi collaboratori probabilmente siano già nel cloud, è possibile che una parte sia disponibile solo all'interno della rete aziendale. In genere i lavoratori in remoto utilizzano una rete privata virtuale (VPN) per collegare in modo sicuro i propri computer portatili Windows o macOS e i dispositivi mobili Android o iOS su internet, attraverso i firewall.

Connessione dei lavoratori in remoto ad applicazioni e dati interni

Le funzionalità VPN complete sono già integrate in Forcepoint NGFW
Se devi consentire l'accesso VPN a utenti che non hanno mai lavorato in remoto, o se si verificano problemi con la soluzione VPN esistente, Forcepoint NGFW è dotato di funzionalità VPN complete integrate; non è necessario acquistare licenze aggiuntive. Con il nostro portale SSL VPN puoi offrire agli utenti una connettività facile e sicura alle applicazioni web interne, accessibili tramite il loro browser e senza alcun software client particolare per gli endpoint.

Altrimenti, per gli amministratori che necessitano di un accesso di rete completo, è possibile scaricare il nostro software client VPN per Windows e macOS dalla pagina web support.forcepoint.com. Questi client VPN sono facili da configurare e connettere a Forcepoint NGFW.

Protezione dei carichi di lavoro delle app da migrare nel cloud
Quando si spostano i dati aziendali dai sistemi interni ai carichi di lavoro in ambienti cloud pubblici, ad esempio Microsoft Azure o Amazon Web Services (AWS), le versioni software virtuali di Forcepoint NGFW sono in grado di impedire l'accesso non autorizzato da altre parti di internet. Questi dispositivi virtuali vNGFW, disponibili nei marketplace di Microsoft e Amazon sul cloud pubblico, sono gestiti dal Forcepoint Security Management Center (SMC) allo stesso modo dei dispositivi fisici, utilizzando anche gli stessi criteri, gli stessi report e le stesse dashboard.



Forcepoint

forcepoint.com/contact

Informazioni su Forcepoint

Forcepoint è un partner strategico per la sicurezza informatica. La sua missione è tutelare le aziende e guidare la trasformazione digitale e la crescita. In luogo di un approccio indifferenziato, che soffoca l'innovazione e crea vulnerabilità, Forcepoint è in sintonia con il modo in cui le persone interagiscono con i dati, fornisce un accesso sicuro e, allo stesso tempo, consente ai dipendenti di creare valore. Dalla sua sede ad Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di aziende private e pubbliche in più di 150 paesi.

Scopri di più su Cloud Security al link forcepoint.com/cloud-security